



Calhoun: The NPS Institutional Archive
DSpace Repository

Theses and Dissertations

1. Thesis and Dissertation Collection, all items

2009-12

Fusion center privacy policies : does one size fit all?

Harper, Jennifer L.

Monterey, California. Naval Postgraduate School

<http://hdl.handle.net/10945/4431>

Copyright is reserved by the copyright owner.

Downloaded from NPS Archive: Calhoun



Calhoun is the Naval Postgraduate School's public access digital repository for research materials and institutional publications created by the NPS community. Calhoun is named for Professor of Mathematics Guy K. Calhoun, NPS's first appointed -- and published -- scholarly author.

Dudley Knox Library / Naval Postgraduate School
411 Dyer Road / 1 University Circle
Monterey, California USA 93943

<http://www.nps.edu/library>



NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

**FUSION CENTER PRIVACY POLICIES:
DOES ONE SIZE FIT ALL?**

by

Jennifer L. Harper

December 2009

Thesis Advisor:
Second Reader:

John Rollins
Michael Petrie

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			<i>Form Approved OMB No. 0704-0188</i>	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.				
1. AGENCY USE ONLY (Leave blank)		2. REPORT DATE December 2009	3. REPORT TYPE AND DATES COVERED Master's Thesis	
4. TITLE AND SUBTITLE Fusion Center Privacy Policies: Does One Size Fit All?			5. FUNDING NUMBERS	
6. AUTHOR(S) Jennifer L. Harper				
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			10. SPONSORING/MONITORING AGENCY REPORT NUMBER	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. government.				
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited			12b. DISTRIBUTION CODE A	
13. ABSTRACT (maximum 200 words) The <i>9/11 Commission Report</i> states, "The choice between security and liberty is a false choice, as nothing is more likely to endanger America's liberties than the success of a terrorist attack at home. Our history has shown us that insecurity threatens liberty. Yet, if our liberties are curtailed, we lose the values that we are struggling to defend." This thesis will explore privacy policies from established fusion centers, federal guidance and civil liberty advocate statements on privacy, civil liberty infringement and the sharing of information in and outside of fusion centers. Recommendations are provided for the State of New Hampshire's Information and Analysis Center as the basis for developing a privacy and civil liberty policy framework that maintains the integrity of the information, protects citizens' rights, and achieves the mission of the center.				
14. SUBJECT TERMS Fusion center, privacy policy, civil liberties, information and analysis center, New Hampshire			15. NUMBER OF PAGES 117	
			16. PRICE CODE	
17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT UU	

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. Z39-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

FUSION CENTER PRIVACY POLICIES: DOES ONE SIZE FIT ALL?

Jennifer L. Harper
Bioterrorism Coordinator,
New Hampshire Homeland Security and Emergency Management
B.A., Franklin Pierce College, 1995
M.B.A., Southern New Hampshire University, 2002

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)**

from the

**NAVAL POSTGRADUATE SCHOOL
December 2009**

Author: Jennifer L. Harper

Approved by: John Rollins
Thesis Advisor

Michael Petrie
Second Reader

Harold A. Trinkunas, PhD
Chairman, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The *9/11 Commission Report* states, “The choice between security and liberty is a false choice, as nothing is more likely to endanger America’s liberties than the success of a terrorist attack at home. Our history has shown us that insecurity threatens liberty. Yet, if our liberties are curtailed, we lose the values that we are struggling to defend.” This thesis will explore privacy policies from established fusion centers, federal guidance and civil liberty advocate statements on privacy, civil liberty infringement and the sharing of information in and outside of fusion centers. Recommendations are provided for the State of New Hampshire’s Information and Analysis Center as the basis for developing a privacy and civil liberty policy framework that maintains the integrity of the information, protects citizens’ rights, and achieves the mission of the center.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I.	INTRODUCTION.....	1
A.	PROBLEM STATEMENT	1
B.	PRIVACY AND CIVIL LIBERTY CONCERNS WITH FUSION CENTERS.....	4
C.	RESEARCH QUESTION	6
D.	FINDINGS AND RECOMMENDATIONS	6
E.	METHODOLOGY	7
F.	SIGNIFICANCE OF RESEARCH	7
1.	Literature Review	7
2.	Future Research Efforts	11
3.	Immediate Consumer/Customer	11
4.	HS Practitioners and Leaders Nationally	11
II.	BACKGROUND	13
A.	FUSION CENTER’S ROLES AND RESPONSIBILITIES	13
B.	NEW HAMPSHIRE REVISED STATUTES ANNOTATED (RSA) CHAPTER 91–A	20
C.	28 CODE OF FEDERAL REGULATION PART 23	22
D.	FAIR INFORMATION PRACTICES.....	23
E.	U.S. DEPARTMENT OF JUSTICE AND HOMELAND SECURITY GUIDANCE.....	24
1.	Fusion Center Guidelines	24
2.	Baseline Capabilities for Fusion Centers.....	25
3.	Information Sharing Environment	25
F.	AMERICAN CIVIL LIBERTIES UNION (ACLU) AND ELECTRONIC PRIVACY INFORMATION CENTER (EPIC).....	27
III.	ANALYZING PRIVACY AND CIVIL LIBERTY POLICIES	33
A.	GEORGIA INFORMATION SHARING AND ANALYSIS CENTER ...	33
B.	COMMONWEALTH (MASSACHUSETTS) FUSION CENTER	39
C.	ARIZONA COUNTER TERRORISM INFORMATION CENTER.....	45
D.	CONSEQUENCES AND RAMIFICATIONS	49
E.	SUMMING IT UP	51
IV.	RECOMMENDATIONS.....	57
A.	WHAT IS A PRIVACY POLICY?	58
B.	PRIVACY BENCHMARKS	59
C.	SETTING THE STAGE FOR NEW HAMPSHIRE	62
V.	CONCLUSION	69
APPENDIX A.	 BASELINE CAPABILITIES—INFORMATION PRIVACY PROTECTIONS	71
APPENDIX B.	 RESOURCES FOR PRIVACY POLICY DEVELOPMENT	75

APPENDIX C. COMPENDIUM OF NEW HAMPSHIRE’S PRIVACY AND SECURITY LEGISLATION.....	77
APPENDIX D. FUSION CENTER MODEL PRIVACY POLICY SAMPLE TEMPLATE (FROM FUSION CENTER MODEL, 2004)	79
APPENDIX E. DEFINITIONS FOR PRIVACY POLICY DEVELOPMENT	85
APPENDIX F. DRAFT NEW HAMPSHIRE INFORMATION AND ANALYSIS CENTER STRUCTURE	89
LIST OF REFERENCES	91
INITIAL DISTRIBUTION LIST	97

LIST OF FIGURES

Figure 1.	Distributed Information Sources within a Fusion Center (From DOJ, 2006, p. 11)	14
Figure 2.	Information Flow and Process (From Carter, 2008, p. 16).....	15
Figure 3.	Intelligence Process (From DOJ & DHS, 2006, p. 19).....	17
Figure 4.	Participating Entities within a Fusion Center (From DOJ & DHS, 2006, p. 13)	18
Figure 5.	GISAC Information Process (From English, 2007).....	36
Figure 6.	CFC Information Flow (From CFC Operations Manual, 2006).....	42
Figure 7.	AcTIC Information Flow (From Forsyth, 2005).....	47
Figure 8.	Proposed New Hampshire Information and Analysis Center Structure (From Pope, 2009)	89

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

Table 1.	Baseline Capabilities (From Department of Homeland Security, Intelligence and Analysis, 2009).....	71
Table 2.	Compendium of New Hampshire’s Privacy and Security Legislation (From Bureau of Justice Statistics, 2003, pp. 114–115).....	77

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

ACLU	American Civil Liberties Union
ACLUM	American Civil Liberties Union Massachusetts
AcTIC	Arizona Counter Terrorism Information Center
ATF	Alcohol, Tobacco and Firearms
CFC	Commonwealth Fusion Center
CFR	Code of Federal Regulations
CHDS	Center for Homeland Defense & Security
CRS	Congressional Research Service
DHS	Department of Homeland Security
DOJ	Department of Justice
DPHS	Division of Public Health Services
EOC	Emergency Operations Center
EPIC	Electronic Privacy Information Center
FBI	Federal Bureau of Intelligence
GAO	Government Accountability Office
GBI	Georgia Bureau of Information
GEMA	Georgia Emergency Management Agency
GISAC	Georgia Information Sharing and Analysis Center
GTIP	Georgia Terrorism Intelligence Program
HSEM	Homeland Security and Emergency Management
HIDTA	High Intensity Drug Trafficking Areas
IAC	Information and Analysis Center
IC	Intelligence Community
ICE	Immigration and Customs Enforcement
ISE	Information Sharing Environment
JTTF	Joint Terrorism Task Force
LEO	Law Enforcement Online
NCISP	National Criminal Intelligence Sharing Plan
NGA	National Governor's Association

NH	New Hampshire
OIG	Office of Inspector General
RSA	Revised Statute Annotated
TCL	Target Capabilities List
TSA	Transportation Safety Agency

EXECUTIVE SUMMARY

A fusion center is defined as a “collaborative effort of two or more agencies that provide resources, expertise and information to the center with the goal of maximizing their ability to detect, prevent, investigate and respond to criminal and terrorist activity” (Fusion Center Guidelines: Developing and Sharing Information and Intelligence in a New Era. U.S. Department of Justice & Department of Homeland Security, 2006). As fusion centers proliferate nationally, privacy advocates and civil liberty groups continue to be concerned with the risks associated with consolidating and sharing information; authorities feel that the benefits outweigh the risks. While fusion centers have incredible possibilities, there has to be vigilance to assure that the all-hazard, all-crime, counter-terrorism activities undertaken at fusion centers do not compromise the Constitution.

There have been numerous guidance documents developed by both the Department of Homeland Security and the Department of Justice to assist states in developing policies and procedures that meet state and federal laws of ensuring the protection and privacy of citizens. Some fusion centers are extremely open with their information practices and share their policies/procedures with the public, yet others do not. This lack of consistency creates disparity among fusion centers as a whole, thus compounding the concerns.

There is an apparent apprehension amongst many privacy advocates that the increased growth in fusion centers may impinge upon citizens’ civil rights, liberties and privacy. Contributing to this issue is the public’s limited understanding of what the fusion process entails. Privacy advocates fear that these centers may become the next iteration of centralized surveillance of citizens. Privacy advocates and civil liberties groups have concerns with the consolidation of threat information processes may include information on individuals that impinge upon their Constitutional rights to privacy. The American Civil Liberties Union (ACLU) has been especially outspoken over the last three years during the early development and implementation of fusion centers. It has

published numerous reports and articles touting them as “part of an incipient de facto domestic intelligence system” (American Civil Liberties Union, 2008b), amongst other things.

An analysis of privacy policies from three established fusion centers (Georgia, Arizona, and Massachusetts), various federal guidance documents and civil liberty advocate literature on privacy, civil liberty infringement and the sharing of information in fusion centers was conducted for this thesis. Recommendations are provided for the state of New Hampshire’s Information and Analysis Center as the basis for developing a privacy and civil liberty policy framework that maintains the integrity of the information, protects citizens’ rights, and achieves the mission of the center.

State and local fusion centers have diverse needs, characteristics, priorities, threats and vulnerabilities, as well as state laws and statutes that have thus far prevented a national fusion center model due to the functional necessity and the inherent nature of state’s rights and perspectives; inclusive of privacy policies. Currently, fusion centers follow different regulations and fall under different authorities. This creates a significant challenge for the federal government, in collaboration with states, to develop a comprehensive framework that is specific enough to address current opposition to privacy impingement, yet remain flexible enough that it could be applicable for utilization nationwide.

ACKNOWLEDGMENTS

This thesis is the culmination of what has been 18 months of intense learning and growth for me in many ways. CHDS afforded me the opportunity to meet many new friends and colleagues. Cohorts 0803 and 0804 are a great group of men and women to whom I am grateful for their professional and personal insights and lively debate(s) throughout the program; I have truly learned a lot from each of you. To my CHDS friends, as well as instructors, thank you for your friendship, wisdom and patience over the last 18 months, I know you are sick of hearing me talk about fusion centers. I will always remember this great learning experience and our memorable times in “Shepherdsville-town-berg-stand,” West Virginia.

Thank you to John Rollins for his invaluable guidance, assistance and suggestions to improve this thesis. John was always there to be the voice of reason when I thought there was no reason, even when he was out of the country. Special thanks to Michael Petrie for his thoughtful comments and operational knowledge of fusion centers that helped to expand my thesis.

Thank you to Christopher Pope and Kathryn Douthett; I would not have been able to participate in this program without their on-going support and encouragement. It has been difficult to balance the competing priorities with floods, tornadoes, H1N1 spring and current responses, the build-out of the Information and Analysis Center and then trying to find time to complete my course work and thesis in a timely manner. Thanks to both of you for the unique opportunity this has afforded me and the future opportunities that are yet unknown ... for any of us. Thank you to my colleagues at HSEM and DPHS for your support as well.

An extra special thank you goes to my family for their support during the last year-and-a-half. I have missed weekends at Maidstone, vacationing in Florida, the ski slopes and many other things far too numerous to mention. To my friends, thank you for your support and mostly for listening to me complain about too much homework, plus this little thing called a thesis; you have all been great and I owe you.

Derek, I am finally done with homework, so let's hit the slopes and have fun before you start college, and you're too busy with homework and, heaven-forbid, a thesis!

I. INTRODUCTION

We have met the enemy and he is us.

—Pogo

The Twin Towers in New York are gone, along with more than 3,000 innocent Americans. The United Airlines Flight 93 crash in Shanksville, Pa; the American Airlines Flight 77 crash into the Pentagon; bombings of the USS Cole, the U.S. Embassies in Africa and the Khobar Towers in Saudi Arabia; the 2005 London Bombings; the Madrid train bombings in 2004 and numerous other acts of terrorism committed by Islamic terrorists—it's an indisputable fact that all these events happened. That the United States has not had another major terrorist strike since September 11, 2001, is not by accident, nor can it be attributed to good luck; rather, it's due to the efforts and hard work of thousands of dedicated Americans who are involved in the counterterrorism effort to thwart attacks on our homeland. (Rogers, 2008, p. 9)

In the post-9/11 era, the United States as a community has called for law enforcement at the federal, state and local levels to increase their partnerships and work closer with all disciplines in order to expand the capacity of the nation to thwart crime and terrorism. Before 9/11, there were only a few states that had fusion centers that coordinated the collection, analysis and sharing of terrorism and law enforcement information. These were predominantly law enforcement centric centers. On August 3, 2007, President George W. Bush signed into law the *Implementing Recommendations of the 9/11 Commission Act of 2007* (9/11 Commission Act) which legally authorized the creation of fusion centers. Since that time, there has been controversy with their mission, oversight, funding and future.

A. PROBLEM STATEMENT

A fusion center is defined as a “collaborative effort of two or more agencies that provide resources, expertise and information to the center with the goal of maximizing their ability to detect, prevent, investigate and respond to criminal and terrorist activity” (DOJ & DHS, 2006, p. 2). The goal of the fusion center “is to rapidly identify emerging

threats; support multidisciplinary, proactive, and community-focused problem-solving activities; support predictive analysis capabilities; and improve the delivery of emergency and nonemergency services” (Department of Justice & Department of Homeland Security [DOJ & DHS], 2006, p. 13). Researchers on fusion centers have suggested that in an ideal world, fusion centers would involve every level and discipline of government, private sector entities and the public to ensure information from all sources is collected, blended, analyzed and evaluated for relevant information on a continual basis. There is no single source for terrorism-related information, as various pieces of information can come through a variety of efforts within the intelligence community: federal, state and local law enforcement; fire service; emergency management; health and other government entities, as well as private sectors such as energy, transportation and healthcare. Fusion centers afford the opportunity for collaboration of information from such diverse sources.

A fusion center is not a traditional intelligence center, nor is it an emergency operations center (EOC); it is a support center that may contain aspects of each of these organizations and is analysis driven. Both an intelligence center and an EOC have specific missions, goals and priorities yet must work together to understand, collaborate and enhance the information-sharing process. There is no single model for a fusion center due to the diverse needs and environmental characteristics of each state that affects the structure, processes and products of a center. A Congressional Research Service (CRS) report published in January 2008 stated that 40 percent of fusion centers labeled themselves as “all-crime” centers, while another 40 percent labeled themselves “all-hazards” as well as “all-crimes” (Rollins, 2008). The definitions of these terms were not consistent amongst the centers, which furthers the lack of a unified fusion center model across the nation. However, regardless of the definition, fusion centers enhance states’ abilities to collect, analyze and share information—intel—domestically. State and local law enforcement officers, who are adequately equipped, trained and fully integrated into an information and intelligence-sharing network, can be invaluable assets in efforts to assist in identifying and apprehending suspected terrorists. An example of this training is

in Arizona, where fusion center personnel train local law enforcement to recognize signs of potential terrorist activity and the significance of relating that information back to the fusion center for further analysis.

Former Assistant Director of Central Intelligence for Analysis and Production, Mark Lowenthal, differentiates *intelligence* from *information* in the following way:

Information is anything that can be known, regardless of how it is discovered. Intelligence refers to information that meets the stated or understood needs of policy makers and has been collected, processed, and narrowed to meet those needs. Intelligence is a subset of the broader category of information. Intelligence and the entire process by which it is identified, obtained, and analyzed respond to the needs of policy makers. All intelligence is information; not all information is intelligence. (2006, p. 1)

The 9/11 Commission Act makes extensive recommendations, from its findings, for changes that can be made to help prevent a similar attack to the homeland in the future. Amongst other things, it specifically calls for a national intelligence chief, a counterterrorism center and increased information sharing. The report states, “the system of ‘need to know’ should be replaced by a system of ‘need to share.’” This directly correlates to fusion centers, which were officially created by the Act. The Act directs the Department of Homeland Security (DHS) to engage and partner with fusion centers in various ways. DHS’s vision of embedding officers from the Office of Intelligence and Analysis (I&A) in fusion centers will allow the states to access DHS information sharing systems. (National Commission on Terrorist Attacks upon the United States [9/11 Commission], 2007) It will also provide them with 24/7 direct access to I&A’s Intelligence Watch and Warning Division, which can provide states with the latest threat information on a nationwide basis. Conversely, DHS officers in the fusion centers can provide infrastructure and analytical context to information, augment the analytical capabilities of fusion centers and provide real-time situational awareness to DHS in times of crisis. Depending on the centers’ construct and maturity, these capabilities may or may not be realized. DHS is optimistic that with further I&A, analysts embedded with the states, and the release of the baseline capabilities document as a guiding principle, that their vision will come to fruition.

B. PRIVACY AND CIVIL LIBERTY CONCERNS WITH FUSION CENTERS

The notion of what privacy is and what is covered differs depending upon the situation and context, but it can include things such as a person's values, behavior, data (personally identifiable), health and their communication and transportation methods. Merriam-Webster defines privacy as "the quality or state of being apart from company or observation" and "freedom from unauthorized intrusion" (Merriam Webster Editorial Staff, 2003). These areas are broad in scope and create cause for concern among privacy advocates, particularly when related to the intelligence cycle that fusion centers follow. One of the many responsibilities fusion centers need to balance is the (privacy) rights of citizens and the task of information collecting and sharing in order to prevent crime and terrorism in the homeland. The U.S. House of Representatives report *Wasted Lessons of 9/11* states:

For fusion centers to be effective, they must not only have adequate resources but also rigorous privacy and civil liberties protections built into their procedures and activities. Without these safeguards, the public will rightly become wary of or even outright opposed to them. (2008, p. 27)

The fusion process inherently allows for the modification of current data with new data in order to provide actionable knowledge/intelligence for multiple disciplines.

There are concerns among many privacy advocates that the increased growth in fusion centers may impinge upon citizens' civil rights, liberties and privacy. Contributing to this fact is the public's limited understanding of what the fusion process entails. Privacy advocates fear that these centers may become the next iteration of centralized surveillance of citizens. Privacy advocates and civil liberties groups are concerned that the risks of consolidating threat information processes may include information on individuals that impinge upon their constitutional rights to privacy.

Opponents of fusion centers, such as the American Civil Liberties Union (ACLU), Electronic Privacy Information Center (EPIC) and the Cato Institute have been outspoken over the last three years during the early development and implementation

phases. They have published numerous reports and articles touting fusion centers as “part of an incipient de facto domestic intelligence system” (American Civil Liberties Union [ACLU], 2008b.), among other things.

As federal data collection and analysis programs become fully functional and accessible by fusion centers, some privacy advocates might see this as a devolution of national intelligence capabilities from the federal government to state government. Some are also concerned that as fusion centers and the intelligence community (IC) agencies codify relationships, there is an increased potential for misuse of private sector data (Massee, O’Neil & Rollins, 2007).

There are concerns by the ACLU and other privacy entities with having DHS performing a coordinating role at the federal level with respect to these centers. According to Masse et al., “We are granting extraordinary powers to one agency, without adequate transparency or safeguards, that hasn’t shown Congress that it’s ready for the job” (2007, pp. 11–12).

ACLU Senior Legislative Counsel, Tim Sparapani, stated, “DHS has begun a downward spiral that continues to strip away individual privacy and rights, as well as trample the sovereignty of the states” (ACLU, 2008a). The ACLU has made recommendations to help preserve privacy, with what it says will not endanger security of the nation but protect citizen rights. It encourages state legislatures to create checks and balances on fusion centers to ensure that mission and objectives are proper.

Cato Institute Director of Information Policy Studies, Jim Harper, stated “Further federal incursion into decentralized, state- and locality-based law-enforcement experience and expertise would be a mistake” (Harper, 2007).

The value of fusion centers is clear, by integrating the various streams of information and intelligence from federal, state and local resources, as well as the private sector, a more accurate picture of risks to people, the economy, infrastructure and communities can be developed and translated into actionable measures. While fusion

centers have incredible possibilities, there has to be vigilance to assure that the all-hazard, all-crime and counter-terrorism activities undertaken at fusion centers do not compromise the Constitution.

The fusion center approach poses potential privacy and constitutional implications; however, these implications have not been fully explored either in principle or in practice. It is an appropriate time to stop, review those operational fusion centers currently deployed and evaluate how they operate and what they actually do and then follow the trail through the legal impact on those issues and make adjustments, where necessary, in an effort to prevent another terrorist attack on the nation.

C. RESEARCH QUESTION

What recommendations can be provided to the New Hampshire Information and Analysis Center (NH IAC) to develop a privacy and civil liberty policy framework that maintains the integrity of the information, protects citizen's rights and achieves the mission of the center, which is to provide actionable intelligence to the right people, at the right time and for the right purpose?

D. FINDINGS AND RECOMMENDATIONS

Research conducted in order to answer the thesis question provided significant findings in the fusion center privacy and civil liberty privacy policy protections. There are centers with successful policies, some with purported violations and still others with substantiated violations of their policies.

The federal government has developed a wealth of information and guidance for states to utilize in the creation of a privacy policy for their fusion center. One such document is the *Baseline Capabilities for State and Major Urban Area Fusion Centers: A Supplement to the Fusion Center Guidelines* (Department of Justice and Department of Homeland Security [DOJ & DHS], 2008), which outlines five specific privacy requirements for centers to achieve in order to meet the identified baseline requirements.

These recommendations and others are outlined in Chapter IV to provide assistance in the development a privacy policy, not only for the NH IAC, but also for other centers that may be at the same point or for those considering a revision of their privacy policy.

E. METHODOLOGY

The methodology to be utilized for this thesis will be case studies that specifically review established fusion center privacy and civil liberty programs. The case studies will focus on privacy and civil liberty documents from Georgia, Massachusetts and Arizona. These state fusion centers have been established for several years and are viewed by DHS and states as examples of model practices for fusion center development. By reviewing each state's program against federal guidelines and defining gaps, lessons can be learned in order to make appropriate (policy) recommendations to address those challenges facing New Hampshire's Information and Analysis Center, as well as fusion centers nationwide, regarding privacy and civil liberty concerns by the ACLU and other privacy organizations.

F. SIGNIFICANCE OF RESEARCH

1. Literature Review

Substantial work has been done to establish minimum guidelines and standards for addressing privacy issues in fusion center operations. Nonetheless, critics and public opinion, in general, suggest that there is a lack of trust that the policies are truly effective to comprehensively protect privacy and civil liberties rights. This thesis will delve into effective privacy and civil liberty policy frameworks, and how an effective framework can be implemented while still maintaining the integrity of the information and the mission of the fusion center.

State and first responders who are adequately equipped, trained and fully integrated into an information and intelligence-sharing network can be invaluable assets in efforts to assist in identifying and apprehending suspected terrorists. According to the

National Criminal Intelligence Sharing Plan, “Sharing is founded upon trust between the information provider and the intelligence consumer. Such trust is most often fostered on an interpersonal basis; therefore, law enforcement task forces and other joint work endeavors succeed where collocated, interspersed personnel from different agencies and job types convene for a common purpose.” (Global Justice Information Sharing Initiative [Global], 2003, p .9).

The creation of state and local fusion centers has caused advocacy groups to raise questions about privacy and civil liberties that are being compromised, information being used inappropriately and unnecessarily and questioning the unknown manner in which information is collected, stored and disseminated. Fusion centers have taken steps to ensure privacy and civil liberties are protected by developing multidisciplinary governance structures, including external oversight, the development of policies and procedures and the adoption and adherence to 28 Code of Federal Regulations (CFR) Part 23, developing audit checklists, and adherence to applicable state and federal constitutional and statutory privacy and civil liberties provisions. The National Research Council states, “Privacy is, and should continue to be, a fundamental dimension of living in a free, democratic society” (2008, p. 9) and that “Even under the pressure of threats as serious as terrorism, the privacy rights and civil liberties that are the cherished core values of our nation must not be destroyed” (2008, p. 4).

Questions will arise for fusion center officials when attempting to balance and understand privacy interests while collecting, aggregating and disseminating information. For example: what will the information be used for, where does the information come from and what are the consequences for the individual whose information is at issue? According to Gregory Treverton, “In principle, effects on privacy and civil liberties should be determined by the *mission and rules* governing collecting, storage, and sharing of information, not on the *design* of the organization doing the collecting and storing” (2008, p. xviii).

Literature published related to privacy and civil liberty concerns of state fusion centers is varied from both the government and privacy advocate perspectives. Literature

sources can be grouped as follows: government documents/guidelines/resources, Congressional Research Service and best practice reports, privacy and civil liberty documents/articles/research and independent polls/research.

Substantial oversight regarding the operation of fusion centers is already in place. However, shortfalls exist about the assessment of existing privacy and civil liberty programs that review policy, resource and organizational implications and considerations against federal guidance. The federal government has developed extensive guidelines and resource frameworks for fusion centers regarding protecting privacy and other issues. There are challenges related to how the guidance will be implemented, as well as the roles, responsibilities and accountability assignments for the participants. The *State Fusion Center Processes and Procedures: Best Practices and Recommendations* states, “Independent oversight is a valuable management function that should be sought and welcomed” (Rollins & Connors, 2007, p. 8). They also state, “It is in the best interest of the center to have an independent authority validate that the center is operating within constitutional and legal limits and that appropriate accountability actions are taken when mistakes are discovered” (Rollins & Connors, 2007, p. 8).

The U.S. Department of Justice (DOJ), Office of Justice Programs, Bureau of Justice Assistance, in collaboration with DOJ’s Global Justice Information Sharing Initiative and the U.S. Department of Homeland Security 2006, have developed and issued the *Fusion Center Guidelines: Developing and Sharing Information and Intelligence in a New Era*. According to the Hugo Teufel, Chief Privacy Officer for DHS, “These guidelines are intended to ensure that fusion centers are established and operated consistently, resulting in enhanced coordination, strengthened partnerships and improved crime-fighting and anti-terrorism capabilities” (2007, p. 4). There are specific guidelines in the document that discuss the development of a comprehensive privacy policy. Recommendations suggest that fusion centers complete privacy impact assessments to understand the effect that technology and operational choices have on privacy and contribute to enhanced protections. While the federal government does not mandate these guidelines, all fusion centers have agreed to follow them, to-date.

DHS Chief Privacy Officer, Hugo Teufel testified that:

Implementing these fusion center guidelines provides an important first step in applying appropriate privacy protections as required under the “Guidelines to Ensure that the Information Privacy and other Legal Rights of Americans are Protected in Development and use of the Information Sharing Environment.” (2007, p.3)

The U.S. Intelligence Reform and Terrorism Prevention Act of 2004 emphasizes the prevention of terrorism through the sharing of information and a structured, information-sharing environment formalizes the establishment of state fusion centers. Although the Information Sharing Environment (ISE) Privacy Guidelines are not applicable to state or local fusion centers, federal entities must ensure that any information shared with fusion centers have privacy protection guidelines that are at least as comprehensive as the ISE guidelines. States are well served by utilizing the ISE guidelines as a starting point. This approach replicates efforts that have already been scrutinized and may shield future fusion centers from criticism of advocacy groups.

The most recent federal document addressing fusion centers is the *Baseline Capabilities for State and Major Urban Area Fusion Centers: A Supplement to the Fusion Center Guidelines*. The document assists fusion centers in the identification, prioritization and allocation of resources necessary to achieve baseline levels of capability based on locally identified needs. When a center achieves this baseline, it will have the essential structures, processes and tools available to support gathering, processing, analyzing and disseminating terrorism, homeland security and law enforcement information for all levels of government and the private sector, where appropriate. Terrorism and criminal activity are frequently related, therefore, analyzing them simultaneously is prudent.

Civil liberty groups such as the American Civil Liberties Union, the Electronic Privacy Information Center (EPIC) and the Cato Institute have been candid with their opinions about the concept of fusion centers prior to 9/11; they do not like them. Lillie Conley stated:

Investigations conducted by the Congressional Research Service, ACLU, EPIC, and others raise more questions than are answered about the real world implications of the Department of Homeland Security's role in the development of intelligence fusion centers. EPIC concluded that Intelligence fusion center development and implementation is unfocused and undirected. (2007, p .9)

States have the mechanisms and capabilities to protect citizen's rights and it is up to each state to ensure it does so within the context of state, local and federal laws as well as the constitution.

2. Future Research Efforts

The significance of this research will assist in the creation of a privacy and civil liberty program for New Hampshire's Information and Analysis Center through the recommendations of comprehensive policies and procedures. This thesis will also outline recommendations that may influence the U.S. Department of Homeland Security to institute changes in federal guidance to state and local fusion centers.

3. Immediate Consumer/Customer

The immediate consumer or customer of this research will be the New Hampshire Department of Safety, Homeland Security and Emergency Management to utilize in the establishment of the New Hampshire Information and Analysis Center.

4. HS Practitioners and Leaders Nationally

The research will assist practitioners in Homeland Security and Fusion Centers to understand the necessary requirements to have a solid privacy and civil liberty program that satisfies the needs of the local and state government, in addition to privacy groups concerned with civil liberty rights.

The next section of this thesis will provide background and context for the reader on some of the issues and obstacles of privacy policies, which will then lead into a discussion of the importance and implications of privacy policies for fusion centers.

THIS PAGE INTENTIONALLY LEFT BLANK

II. BACKGROUND

The right to be let alone is indeed the beginning of all freedom.

—William Orville Douglas, U.S. Supreme Court

A. FUSION CENTER’S ROLES AND RESPONSIBILITIES

The fusion center is focused on information collection, integration, evaluation, analytic processes and the distribution of enhanced information to its constituents. This is all completed through the fusion process which “refers to the overarching process of managing the flow of information and intelligence across all levels and sectors of government and private industry ... supports the implementation of risk-based, information-driven prevention, response, and consequence management programs” (DOJ & DHS, 2006, p. 3). One of the primary missions of a fusion center is information sharing, which Figure 1 illustrates broadly. The Fusion Center Guidelines state:

Users access the data via a common interface, extracting, analyzing, and disseminating information based on need and current demands. Although it is anticipated that fusion and fusion centers will primarily be used for preventive and proactive measures, the process will also be critical if an incident occurs, providing information to responders as well as officials, media, and citizens.” (DOJ & DHS, 2006, p. 11)

This process affords all participating entities with the ability to provide and receive synthesized information.



Figure 1. Distributed Information Sources within a Fusion Center
(From DOJ, 2006, p. 11)

As the fusion center concept relies on numerous entities with varying responsibilities and capabilities in operationalizing a fusion center, one of the essential objectives is to gain “buy-in” from all the key stakeholders in the state. Figure 2 illustrates the flow and processing of information within a fusion center.

The concept depicted is that the information is received as raw data and intelligence from various entities, analysts then integrate the diverse data and provide analytic output that may include, but not be limited to, information to prevent an incident,

identification of the need to harden a facility or it may identify the need to conduct a threat assessment. This is all referred to in the fusion process as actionable intelligence.

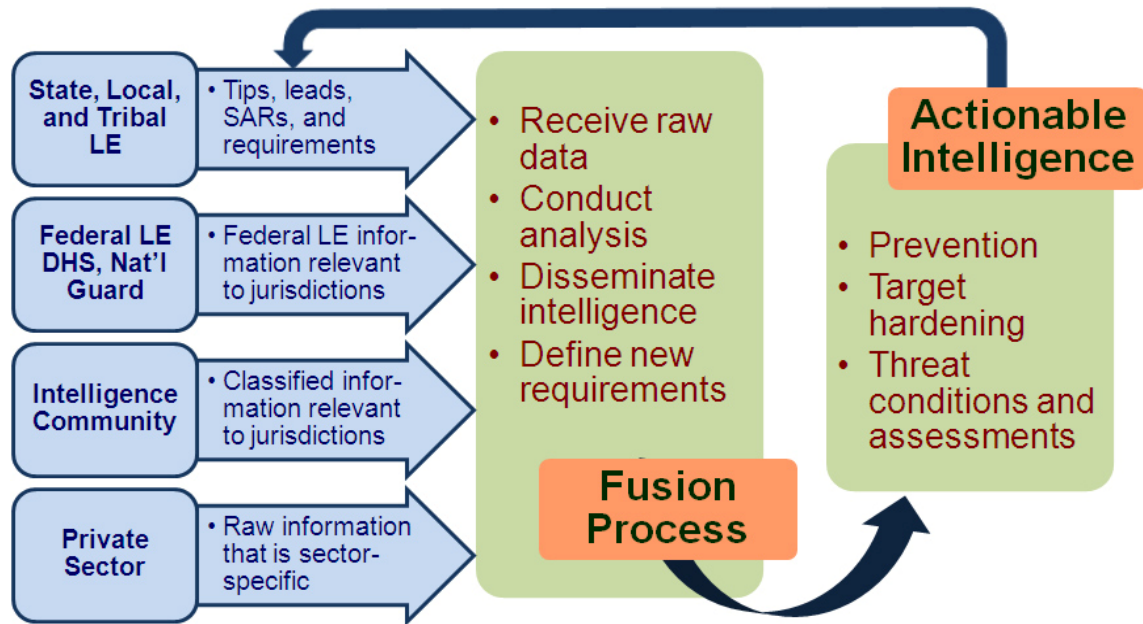


Figure 2. Information Flow and Process (From Carter, 2008, p. 16)

Effective all-hazard, all-crime and counterterrorism related prevention, protection, preparedness, response and recovery efforts depend on timely and accurate information. This information covers a wide range of topics, such as weather events that may cause damage and/or injury, where crimes are committed and on the counter-terrorism side, who the enemy is, where they operate, how they are supported, their intended target and the method of attack.

According to the Fusion Center Guidelines, “a fusion center is an effective and efficient mechanism to exchange information and intelligence, maximize resources, streamline operations, and improve the ability to fight crime and terrorism by analyzing data from a variety of sources” (DOJ & DHS, 2006, p. 2.). Additionally, the Guidelines state, “Fusion centers embody the core of collaboration, and as demands increase and resources decrease, fusion centers will become an effective tool to maximize available resources and build trusted relationships” (DOJ & DHS, 2006, p. 4.)

The U.S. Department of Justice and Department of Homeland Security *Baseline Capabilities for State and Major Urban Area Fusion Centers* states:

While it is acknowledged that the Intelligence Process is different from the Fusion Process, the basic foundational steps of the intelligence process can be applied to identifying the baseline capabilities fusion centers should strive to achieve in regards to information and intelligence collection, collation, analysis and dissemination. (2008, p. 9.)

The intelligence process involves a series of steps as outlined in Figure 3. This illustrates a professional and dynamic approach to identify and counter threats, utilizing intelligence assets and functions. The desire is for this process to be objective, unbiased, without prejudice, and it must be based on accurate and relevant facts with due consideration for the privacy and constitutional rights of individuals, groups and organizations. The intelligence process can be realized as a series of decision-making points, with each point requiring a decision to be made from several alternatives, with each resulting with their own consequence—positive or negative. The adoption of a policy that addresses the protection of individual privacy and constitutional rights and attempts to eliminate unnecessary discretion in the decision-making process, guide the necessary discretion and ensure conformance with the policy goal(s) is an optimal outcome of this process.



Figure 3. Intelligence Process (From DOJ & DHS, 2006, p. 19)

Some security experts indicate that the lack of a national model for developing fusion centers is a mistake. The fact that state and local fusion centers have diverse needs, characteristics, priorities, as well as state laws may prevent a national model due to the functional necessity and the inherent nature of states' rights and perspectives. This may not be a mistake. Entities within fusion centers will vary due to their functional configuration. Figure 4 outlines this collaborative nature. Fusion centers "focus on collaboration and analysis and will become a repository for information that flows through the center, while ensuring state and federal privacy laws and requirements are adhered to" (DOJ & DHS, 2006, p. 13).

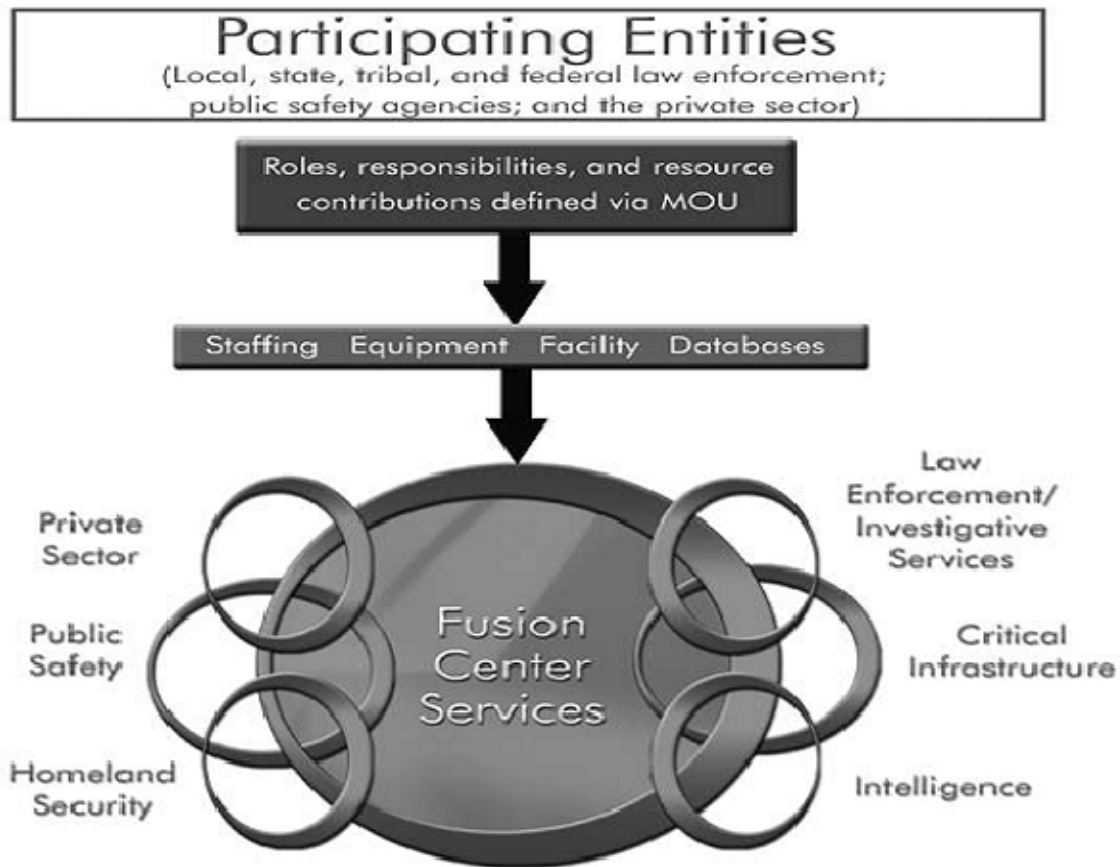


Figure 4. Participating Entities within a Fusion Center
(From DOJ & DHS, 2006, p. 13)

Multiple strategies and technologies must be developed for diverse two-way information sharing to capture information from non-traditional stakeholders and to provide threat-based intelligence and intelligence requirements back to those who have the need to know. A lack of information sharing and ability to provide timely and actionable intelligence were identified failures of 9/11. Between and among all the reports, commissions, white papers, books and array of other literature and lessons learned in the eight years since 9/11, it should be realized by those in the intelligence community that there is value added in working in partnership with a cross-section of diverse stakeholders to ensure the safety and security of U.S. citizens. The more information that is communicated between and amongst all stakeholders, the more knowledgeable the community at large becomes on the subject matter—whether it is criminal, all-hazard or counter-terrorism in nature. Masse et al., “The

rise of fusion centers is representative of a recognition that non-traditional actors—state and local law enforcement and public safety agencies—have an important role to play in homeland defense and security” (2007, p. 2). With the desire to further communications and the flow of information, comes the need to be acutely aware of the issues of privacy and civil liberties and protection of information. The National Strategy for Information Sharing states:

Protecting the rights of Americans is a core facet of our information sharing efforts. While we must zealously protect our Nation from the real and continuing threat of terrorist attacks, we must just as zealously protect the information privacy rights and other legal rights of Americans. With proper planning we can have both enhanced privacy protections and increased information sharing. (2007, p. 27)

It is important to note that with the rise of fusion centers across the nation and value-added that they bring to the entities involved in them, not every state has bought into the concept to-date. About two years ago, the state of New Hampshire started to engage various stakeholders within state government on the applicability and feasibility of establishing a center. The New Hampshire Information and Analysis Center (IAC) will serve as the statewide nucleus for information collection, analysis and dissemination of all-hazard, all-crime and counter-terrorism threats to the state. The current plan, as outlined in the New Hampshire Emergency Management Preparedness Grant (EMGP) work plan, is to develop resources to provide secure information sharing as well as information collection for the purposes of developing intelligence for its stakeholders (New Hampshire Homeland Security and Emergency Management, 2008). The IAC plans to support local entities with access to federal information sources and restricted databases as well as analytic services to support complex incidents, as appropriate, through such means as the Homeland Security Information Network (HSIN), Homeland Secure Data Network (HSDN), Homeland Security State and Local Intelligence Community (HS SLIC) and an array of others. Access to certain information will be restricted based on a need to know and right to know as required by New Hampshire state statutes, the New Hampshire Constitution and 28 CFR Part 23. Once the IAC is operational, actionable intelligence products will be provided to local stakeholders based upon the defined threat made from ongoing assessments and information and intelligence

needs defined by the stakeholders. David Carter, author of *Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies*:

The four greatest challenges are: 1. Develop a cooperative and committed relationship between all stakeholders; 2. Ensure privacy and protection of personal identifying information; 2. Establish policies and process that support efficient, effective and lawful intelligence operations; and 4. Stay on message as an analytic center. (2009, p.195)

Officials in New Hampshire have had discussions with privacy advocates, as well as legislators on these very issues already. They will be area's requiring constant focus and attention as the process to build out the IAC moves forward. The New Hampshire Department of Safety worked closely with these groups and put forth legislation to create the IAC in the 2008 session. The bill passed the House but died in the Senate for reasons unknown to this author. The Department has met several times since with the legislator to discuss furthering the IAC and, more specifically, regarding privacy and civil liberty rights of New Hampshire citizens and the importance of transparency and the assurance of these rights as the IAC moves forward.

As fusion centers expand and disciplines work closer with each other, they begin to create a synergy. If each of them has a piece of the puzzle and work as a team, the puzzle can be put together by working smarter, not harder. This is true for New Hampshire as well, in that there are only so many resources (personnel), so optimizing time, skills and energy will maximize those resources to the fullest potential through the team approach.

B. NEW HAMPSHIRE REVISED STATUTES ANNOTATED (RSA) CHAPTER 91-A

The Right-To-Know law balances the citizens' rights-to-know with right to keep certain aspects of their interactions with government and certain personal information the government maintains on them private. This law dissects all components of state government—unless otherwise annotated.

Revised Statutes Annotated (RSA) 91-A:1 Preamble states, "Openness in the conduct of public business is essential to a democratic society. ...ensure both the greatest

possible public access to the actions, discussions and records of all public bodies, and their accountability to the people” (New Hampshire Revised Statutes Annotated [NHRSA], 1977). This law provides a clear, concise outline of citizens’ rights within the context of public meetings and their ability to request governmental records and information from such. There are exemptions outlined in 91-A:5-VI that relate specifically to “...matters relating to the preparation for and the carrying out of all emergency functions...developed by local or state safety officials that are directly intended to thwart a deliberate act that is intended to result in widespread or severe damage to property or widespread injury or loss of life” (NHRSA, 2008b). This section protects those discussions that directly related to terrorism, which include any planning documents. This information in the wrong hands could potentially jeopardize the safety, security and economy of New Hampshire’s citizens, visitors and businesses.

RSA 91-A allows for certain law enforcement investigate records to be disclosed. If the records requested are either investigative records or compiled for law enforcement purposes, they may be withheld if the law enforcement agency can prove that disclosure meets specific requirements outlined in the RSA. Other confidential information utilized by law enforcement officers in their duty to safeguard citizens is protected under 28 CFR 23. This provision and 28 CFR 23 provides for the protection of information that is of criminal nature and under investigation; disclosure of this information could be detrimental to the on-going case investigation.

New Hampshire’s Right-to-Know Law guarantees that its citizens have reasonable access to public meetings and records. Additionally, New Hampshire’s Constitution also guarantee’s accountability to its citizens as stated in Part I, Article 8:

All power residing originally in, and being derived from, the people, all the magistrates and officers of government are their substitutes and agents, and at all times accountable to them. Government, therefore, should be open, accessible, accountable and responsive. To that end, the public’s right of access to governmental proceedings and records shall not be unreasonably restricted.” (NH Constitution, Amended, 1976)

New Hampshire after all, is the “Live Free or Die” state, and its citizens expect and enjoy the freedoms that democracy allows for to the fullest extent possible. They want to be informed and involved yet protected—that is, the balance that must be weighed.

Appendix C is a “Compendium of New Hampshire’s Privacy and Security Legislation” that outlines New Hampshire’s state laws and regulations relating to privacy and security of criminal history record information. According to the Department of Justice, Bureau of Justice Statistics, “...the compendia are intended to promote the evolution of enlightened privacy and information policy” (2003, p. 1).

C. 28 CODE OF FEDERAL REGULATION PART 23

The U.S. Department of Justice established this regulation to assure that all criminal intelligence systems are utilized in conformance with the privacy and constitutional rights of individuals. Many fusion centers typically apply the protections developed for their covered criminal intelligence system for all of their systems, thus, familiarity and compliance with 28 Code of Federal Regulation (CFR) Part 23 serves the fusion centers well as they adopt recommendations of the Information Sharing Environment (ISE). The Department of Safety, as well as local law enforcement agencies in the state, follow 28 CFR Part 23 as part of their normal operating protocols. It is the standard for law enforcement nationwide as it has been vetted, challenged and approved at the highest level of government.

It is important for not only law enforcement but any entity working within a fusion center to know this policy inside and out to ensure compliance at all time. According to 28 CFR Part 23 policy standards:

(1) Criminal Intelligence System or Intelligence System means the arrangements, equipment, facilities, and procedures used for the receipt, storage, interagency exchange or dissemination, and analysis of criminal intelligence information; (2) Interjurisdictional Intelligence System means an intelligence system which involves two or more participating agencies representing different governmental units or jurisdictions; (3) Criminal Intelligence Information means data which has been evaluated to determine that it: (i) is relevant to the identification of and the criminal

activity engaged in by an individual who or organization which is reasonably suspected of involvement in criminal activity, and (ii) meets criminal intelligence system submission criteria; (4) Participating Agency means an agency of local, county, State, Federal, or other governmental unit which exercises law enforcement or criminal investigation authority and which is authorized to submit and receive criminal intelligence information through an interjurisdictional intelligence system. A participating agency may be a member or a nonmember of an interjurisdictional intelligence system; (5) Intelligence Project or Project means the organizational unit which operates an intelligence system on behalf of and for the benefit of a single agency or the organization which operates an interjurisdictional intelligence system on behalf of a group of participating agencies; and (6) Validation of Information means the procedures governing the periodic review of criminal intelligence information to assure its continuing compliance with system submission criteria established by regulation or program policy. (Civil Liberties & Privacy Office, 2008)

D. FAIR INFORMATION PRACTICES

The Organization of Economic Cooperation and Development created eight privacy design principles known as the Fair Information Practices (FIP). These principles are: transparency, individual participation, purpose specification, data minimization, use limitation, data quality and integrity, security, and accountability and auditing; these eight principles are the universal standard for privacy protection. DHS instituted the FIP as its foundation for privacy policy and implementation across the Department in 2008. The principles are highlighted in Guideline 8 of the Fusion Center Guidelines and are reiterated in Section II of the Baseline Capabilities document. (DOJ & DHS, 2008) The FIPs form the basis for privacy compliance policies and procedures governing the use of personally identifiable information. In an era with increasing technology and digitization of individuals' information, having fundamental information practices firmly in place is crucial to a well-balanced, unbiased society.

Critics of FIPs can be found on both sides. Some in the privacy field believe that FIPs are too ineffective, allow too many exemptions, do not require a privacy agency, fail to account for the weaknesses of self-regulation and have not kept pace with the increasing use of information technology. Critics from a business perspective want to

limit FIPs to reduce elements of notice, consent and accountability and complain that other elements are impracticable, costly or not consistent with openness or free speech standards. FIPs were developed to help facilitate the balance between the right to privacy while ensuring the safety of citizens and the ability to discover bad people who want to do bad things before they can implement those kinds of scenarios in the United States.

E. U.S. DEPARTMENT OF JUSTICE AND HOMELAND SECURITY GUIDANCE

The federal government has developed and provided significant guidance and resource frameworks for state and local fusion centers regarding protecting privacy and civil liberties for their citizens. The following information provides background and context for the case studies in Chapter III that focus on privacy policies in established fusion centers.

1. Fusion Center Guidelines

The U.S. Department of Justice and the U.S. Department of Homeland Security developed the all-crime, all-hazard “Fusion Center Guidelines” in August 2006 in an effort “...to ensure that fusion centers are established and operated consistently, resulting in enhanced coordination efforts, strengthened partnerships, and improved crime-fighting and antiterrorism capabilities” (DOJ & DHS, 2006, p. 2). There are 18 guidelines that state and local entities can utilize in the development of a fusion center to ensure consistency and continuity in an effort to share intelligence information across the nation both vertically and horizontally. At a minimum, each guideline has sections for justification of the specific topic, issues for consideration when developing the topic and additional resources for further guidance on the topic. Guideline 8 specifically addresses the development, publication and adherence to privacy and civil liberty policies. The guideline references the “Privacy Policy Development Guide,” “Privacy and Civil Rights Policy Template for Justice Information Systems” and the “Fair Information Practices” as documents and tools to be utilized in developing a Privacy and Civil Liberty Policy (DOJ & DHS, 2006, p. 41). The guidelines are not mandated, they merely provide a starting point for the development of a fusion center privacy policy. Legal counsel will be

required to ensure that it will meet the mark for the specific state in adhering with its constitution, laws and its citizen's right to know about the fusion center mission.

2. Baseline Capabilities for Fusion Centers

The Baseline Capabilities for Fusion Centers, developed by the U.S. Department of Justice and U.S. Department of Homeland Security in September 2008, is a supplement to the Fusion Center Guidelines. This document identifies the baseline capabilities for fusion centers and the operational standards necessary to achieve each of the capabilities. According to the guidance, "By achieving this baseline level of capability, a fusion center will have the necessary structures, processes, and tools in place to support the gathering, processing, analysis, and dissemination of terrorism, homeland security, and law enforcement information" (DOJ & DHS, 2008, p. 1). According to the Baseline Capabilities document, "The achievement of the information privacy protections capabilities will result in a fusion center privacy protection policy that meets the Section 12.d. requirement of the Information Sharing Environment Privacy Guidelines" (DOJ & DHS, 2008, p. 27). From an operational perspective, since each center is unique in its structure, the baseline capabilities provide the flexibility to work within various settings; all crimes, all-hazards and counter-terrorism or a combination of one, two or all three. DHS estimates it could take fusion centers up to five years to achieve all the baseline capabilities, due to varying constraints on and maturity of each fusion center. Once a fusion center reaches the baseline capabilities, it will take focused concentration in order to sustain the center. This is because there will be distractions over funding, governance, privacy and politics, only to mention a few; however, all of these have the potential to obliterate a center if there is not a constant feeding and nurturing of its mission and goals.

3. Information Sharing Environment

Thomas E. McNamara, Program Manager, Information Sharing Environment stated:

Recognizing the need to go beyond individual solutions to create an environment—the aggregation of legal, policy, cultural, organizational, and technological conditions—for improving information sharing,

Congress passed and the President signed the landmark *Intelligence Reform and Terrorism Prevention Act of 2004* (IRTPA). The Act requires the President to establish an Information Sharing Environment (ISE), “for the sharing of terrorism information in a manner consistent with national security and with applicable legal standards relating to privacy and civil liberties.” (Program Manager, Information Sharing Environment, 2006, p. xiii)

ISE priorities focus on facilitating, coordinating and expediting access to protected terrorism information to the intelligence, law enforcement, defense, homeland security and foreign affairs communities. The ISE challenge is to gather all types of data, from all levels of security, including structured and unstructured data and finished intelligence products, and to integrate the data with terrorism information and provide access to that information to everyone in the ISE. The ISE privacy guidelines are not applicable to state or local fusion centers; however, federal entities must ensure that any information shared with fusion centers have privacy protection guidelines that are at least as comprehensive as the ISE guidelines. By utilizing the ISE guidelines, states can meet the federal requirements easily as the approach replicates efforts that have already been scrutinized, therefore, safeguarding fusion centers from criticism of advocacy groups.

The three federal documents described above build upon one another in a sequential process to ensure cohesive, compatible and compliant fusion centers are created across the nation to promote a uniform manner of sharing intelligence information to various disciplines based on the topic and need to know. The sharing of information is vital to ensuring the nation’s security from criminals and terrorist organizations whose intent is to harm the United States. Privacy, civil liberty and information policies must be implemented that will safeguard and strengthen the public’s confidence in an agency’s ability to handle information appropriately. The policies will reinforce support for the agency’s information management efforts in utilizing technology, which will in turn bolster effective and responsible sharing of information that maintains the primary concepts of the justice system in the United States.

F. AMERICAN CIVIL LIBERTIES UNION (ACLU) AND ELECTRONIC PRIVACY INFORMATION CENTER (EPIC)

The two leading opponents of fusion centers are the American Civil Liberties Union and the Electronic Privacy Information Center (EPIC). Both have spent numerous hours and staff time on the topic of fusion centers. Moreover, they have testified before congressional hearings, written articles and posted information on their Web sites downplaying centers' ability to protect citizens' privacy and civil liberties within the confines of the law.

The ACLU has spoken out about the development of fusion centers since their inception. It has published numerous reports and articles claiming them to be "part of an incipient de facto domestic intelligence system" (ACLU, 2008b). In its publication, "*What's Wrong With Fusion Centers*," five specific problems with fusion centers are identified:

- **Ambiguous Lines of Authority.** Overlapping jurisdictions create the potential for manipulation of differing laws to evade accountability.
- **Private Sector Participation.** Fusion centers are incorporating private corporations into the intelligence process, further threatening privacy.
- **Military Participation.** Fusion centers are involving military personnel in law enforcement activities in troubling ways.
- **Data Mining.** Federal fusion center guidelines encourage wholesale data collection and manipulation processes that threaten privacy.
- **Excessive Secrecy.** Public oversight, individual redress and the very effectiveness of fusion centers are threatened by excessive secrecy. (German & Stanley, 2007)

Dr. David L. Carter (2008) counters the ACLU allegations in *The Intelligence Fusion Process*, using very clear terminology as to why each of these five items are not issues and should not be of public concern regarding fusion center operations. Fusion centers may appear somewhat suspicious and secretive to those that do not understand their concept, purpose, mission and goals. According to Carter:

There is a concern among many privacy advocates that the growth of fusion centers will increase the jeopardy to citizens' civil rights, liberties and privacy. ... Complicating this issue is the fact that not understanding the concept of the fusion process, many privacy advocates fear that the centers are the next iteration of centralized surveillance of citizens. (2008, p. 23)

Privacy advocates and civil liberty groups are concerned about the risks associated with consolidating threat information; however, authorities feel the benefits outweigh these risks. Some fusion centers are extremely open with their information practices and share their standard operating procedures with the public; others do not. This lack of consistency creates disparity among fusion centers as a whole, thus compounding the opponents' concerns. The *9/11 Commission Report* (2007) states:

The choice between security and liberty is a false choice, as nothing is more likely to endanger America's liberties than the success of a terrorist attack at home. Our history has shown us that insecurity threatens liberty. Yet, if our liberties are curtailed, we lose the values that we are struggling to defend. (2007, p. 395)

The ACLU, EPIC and other advocates are concerned with private sector entities being incorporated into fusion centers. They infer that the relationship between the fusion center and private entities will lead to unfair business advantages by permitting the utilization of classified information and the potential for legal processes to be circumvented. Ben Bain (2008) stated:

Since 2007 the government has released a series of documents and strategies defining the federal vision for the state and locally-owned and operated centers. ... laid out specific roles for fusion centers in the federal government's information sharing environment that authorities use to exchange terrorism-related data.

Private sector participation in fusion centers is governed by state and federal laws that specify what can and cannot be shared. The private sector(s) are the owners of most of the critical infrastructure in this nation, not the federal, state or local government, which is all the more reason for the inclusion of the private sector in the information-sharing network. Building partnerships with private sector organizations creates an environment of trust that allows the sharing of (appropriate) information that ultimately

ensures the safety and security of U.S. citizens. For example, New Hampshire public safety officials received information from a private sector organization of tampering of its system, and that information was shared with the department that has regulatory over that industry. That department was unaware of the tampering and was extremely pleased to have been notified and subsequently reached out to that organization for further follow-up. This type of information sharing is crucial; private sector infrastructure is relied upon on a daily basis by citizens. Therefore, it is for the good of all that it is protected within the confines of the laws that regulate them.

Advocates have raised concerns with DHS regarding its role of coordinating at the federal level with respect to the centers. There is a perception from some advocates that the federal government is mandating the structure of fusion centers, how they collect, analyze and disseminate information, and what types of information is retained, as well as the duration and purpose. The federal government provides guidance and some funding for the centers, but it does not and cannot mandate the centers operations, which is a state's right and decision to make. Mike German, policy counsel at the ACLU and former FBI agent, has expressed concerns regarding these and other issues associated with fusion centers. The ACLU has made statements to the affect that fusion centers are the federal government's attempt to create a domestic intelligence system (ACLU, 2008b) The New Hampshire IAC is governed by the Department of Safety. The center has plans to request technical assistance from DHS regarding specific topics, such as governance, training and baseline capabilities as it is built out. Decisions about the IAC will be made by the state; DHS does not have the authority to mandate to the state the operation of its center, which New Hampshire fully understands.

EPIC has stated that the federal government is responsible for recommendations to limit open government. It even went so far as to file a Freedom of Information Act (FOIA) request with the Virginia State Police for communication information. Virginia drafted legislation to exempt its databases and records from FOIA requests; EPIC believes this would provide too much protection for the state. EPIC's Lillie Coney (2007) states, "There are reasons to be troubled by the development of fusion centers without clear policy and oversight mechanisms in place."

The ACLU continues to be outspoken on the lack of continuity for privacy policies in fusion centers, Rebecca Bernhardt, ACLU of Texas policy director, stated:

We cannot point to a fusion center that has an ideal privacy policy that ensures that when there is bad information in the fusion center, there is a reliable way of removing it, and that there is a policy in place that protects civil liberties. (Longoria, 2009)

The concept of privacy is broad; it encompasses different personal values and interests. Public support for counterterrorism measures is influenced by people's perceptions of the threat of terror: how they think the government is dealing with terrorism and how these actions affect their civil liberties. Public opinion polls suggest that there is a diminished level of acceptance of surveillance systems and biometric recognition systems, which further suggests the public tends to defend civil liberties more in concept than in specific situations (National Research Council, 2008). If perception is reality, then it is important for government to be as transparent as possible in everything that it does.

New Hampshire's initial efforts to establish an Information and Analysis Center identified the area of privacy and civil liberties as a high priority for planning, training and public outreach due to its work with the legislature. As stated earlier, and because privacy advocates and civil liberties groups are concerned that the risks of consolidating information may include information on individuals that impinges upon their constitutional rights to privacy, this was an easy decision.

The 9/11 Commission Act formally codified and established the fusion center initiative, however, from a national perspective, despite the clear statutory authority, unresolved privacy and civil liberty issues continue to threaten the fusion center initiative and the commitment fusion centers hold in preventing terrorist threats to the nation.

As stated in the *9/11 Commission Report* (2007), the fusion center program initiative falls within the scope of the information sharing environment for the sharing of terrorism, homeland security and law enforcement information between parties at all levels of government. DOJ and DHS have developed guidelines and baseline capabilities to assist fusion centers; however, it is not known how effective and to what extent these

documents are being followed to create state privacy policies. There are additional stand-alone documents that explore policies, resources and organizational issues to implement that assure the protection of privacy and civil liberties. However, the existence of a single comprehensive document to facilitate the consistent development of a state privacy policy would help to ensure a consistent approach in the implementation of the fusion center initiative (9/11 Commission, 2007).

As fusion centers presently follow different regulations and fall under different authorities, the significant challenge for the federal government, working with states, is to develop a comprehensive framework that is specific enough to address current opposition to privacy impingement yet remain flexible enough that it could be applicable for utilization nationwide. By reviewing and documenting existing fusion center privacy frameworks, New Hampshire will be in a more informed position to establish its IAC with an assurance that the products and documents created in the information-sharing environment are grounded with a clear, concise and evaluated privacy and civil liberty program.

THIS PAGE INTENTIONALLY LEFT BLANK

III. ANALYZING PRIVACY AND CIVIL LIBERTY POLICIES

Any change, even a change for the better, is always accompanied by drawbacks and discomforts.

—Arnold Bennett, British novelist

The following chapter will focus on privacy policies from fusion centers in Georgia, Massachusetts and Arizona. These three state fusion centers have been established for several years and are viewed by DHS and others in the homeland security arena as examples of model practices for fusion center development and privacy policies. By reviewing these policies against federal guidelines to identify gaps, if any, lessons can be learned in order to make appropriate (policy) recommendations to address those challenges facing fusion centers nationwide regarding privacy and civil liberty concerns made by the ACLU and other privacy organizations. In New Hampshire, an all-crime, all-hazard, counterterrorism Information and Analysis Center (IAC) is in the development phase. The IAC will be managed by the Department of Safety and staffed with personnel from the Division of Homeland Security and Emergency Management and the Division of State Police. It will include other stakeholders when it becomes operational. It is anticipated that New Hampshire will endeavor to make certain that information sharing will be accomplished in accordance with the state's Constitution, statutes, regulations and other legal and policy requirements, including relevant privacy and civil liberty standards and a clearly defined process for redress. The information synthesized in this chapter attempts to provide guidance to assist with the creation of a privacy policy for the NH IAC and other centers at the same juncture in their process.

A. GEORGIA INFORMATION SHARING AND ANALYSIS CENTER

The Georgia Information Sharing and Analysis Center (GISAC) was established in October 2001 under the oversight of the Georgia Office of Homeland Security. The initial focus of GISAC was to address terrorism and to be the conduit for federal, state and local law enforcement to provide homeland security intelligence; this still remains its

focus eight years later. Its primary mission is to serve as state focal point for collection, analysis, assessment and dissemination of terrorism intelligence relating to Georgia.

The Georgia Office of Homeland Security (GOHS) consists of three components: 1) Homeland Security Task Force; 2) Georgia Emergency Management Agency (GEMA); and 3) Georgia Information Sharing and Analysis Center (GISAC). The Homeland Security Task Force is a committee that advises the Director of GOHS on issues related to homeland security and terrorism. GEMA has six sections—finance, hazard mitigation, operations, public affairs, public assistance and terrorism emergency preparedness and response.

According to a Government Accounting Office report:

GISAC has four sections—law enforcement, criminal intelligence, fire services/hazmat, and emergency management. GISAC has a staff of 27, a majority of whom are from the Georgia Bureau of Investigation due to their focus as an all-crime and counter-terrorism fusion center. Other state and local entities with personnel assigned in the center are the Georgia State Patrol, Georgia Department of Corrections, Georgia National Guard, Georgia Sheriffs' Association, Georgia Fire Chiefs Association and Georgia Association of Chiefs of Police. DHS I&A has two staff assigned to GISAC with overall responsibility of providing technical assistance and sharing information amongst the state, local and federal governments; one Southeast region representative and one intelligence officer. There are no FBI personnel assigned directly to GISAC; however there are two GISAC personnel assigned to the JTTF, which is in the same building as GISAC. This allows for access to FBI systems in a timely manner by GISAC personnel. (GAO, 2007)

The GISAC is the only state-level agency dedicated solely to homeland security, antiterrorism and terrorism center operations—it does not have an all-hazards approach. Because GISAC is co-located with the Federal Bureau of Investigation, it enhances and facilitates the collection of information from local and state sources. They integrate this information into a system that is accessible to homeland security and counter-terrorism intelligence programs in the 159 counties that encompass over 650 municipalities statewide. This provides a statewide network of entities that have access to the most current intelligence information at their fingertips.

In order to facilitate effective communication and dissemination of terrorism-related information/intelligence, GISAC has five programs aimed at fostering productive working relationships with local, state and federal government agencies throughout the state. The programs are:

- Counter Terrorism Task Force, which focuses on the protection of Georgia's citizens, critical infrastructure, and key resources from terrorist attacks, major disasters and other emergencies;
- Georgia Terrorism Intelligence Project, which utilizes a Web-based program to virtually share and exchange terrorism tips and leads, generate GIS maps and share/track assets in real time between GISAC and 6 metro Atlanta law enforcement agencies to-date;
- Southern Shield comprises 13 state homeland security offices organized to exchange best practices, share terrorism-related intelligence and monitor regional terrorism threats;
- Interstate Counter-Terrorism Operations Network is a communications network between GISAC and other fusion centers across the nation to promote information sharing; and lastly,
- Coordinating Operations with the Atlanta FBI Joint Terrorism Task Force, this approach consolidated operational activities of both entities so they receive the same information, leads, research and can investigate cases jointly which provides for a more coordinated and less duplicative system. (Georgia Emergency Management Agency [GEMA], n.d.).

GISAC is also involved with the business and industry sector through a partnership that was formed in 2003 with the Business Executives for National Security (BENS). BENS is a nationwide, non-partisan organization that engages senior business executives to enhance the nation's security by partnering with state emergency management officials.

Governor Sonny Purdue worked with BENS to create the Georgia Business Force (GBF), which became a not-for-profit entity earlier this year. GBF is a non-partisan coalition of critical infrastructure/key resource (CI/KR) companies/associations committed to support Georgia in preparation for and response to disasters and homeland security threats within its borders. The GBF established and currently manages the Business Operations Center, within GEMA, to share information with CIKR entities

during activations of the state emergency operations center. This partnership truly illustrates the cooperative and collaborative commitment that Georgia has to its homeland security, counter-terrorism and CIKR programs and ensuring the safety and security of its citizens (GEMA, n.d.).

Figure 5 outlines the flow of information handling and evaluation at the GISAC.

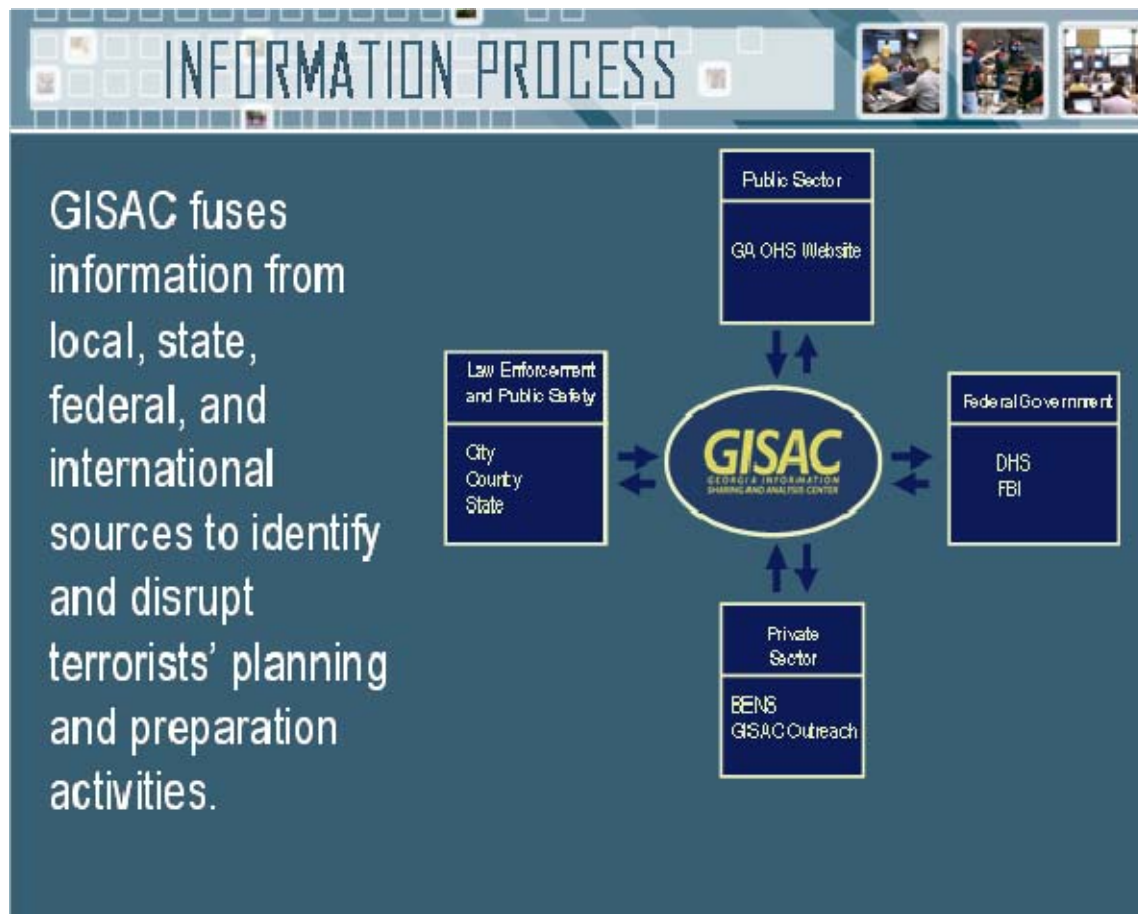


Figure 5. GISAC Information Process (From English, 2007)

Situational awareness briefings are conducted every morning between JTTF and GISAC personnel. The GISAC requires all staff to have security clearances, including secretarial/administrative support staff. GISAC is enhancing its capability and capacity to integrate terrorism emergency response and preparedness to include critical infrastructure protection (CIP); the current connection for CIP is through the Georgia Emergency Management Agency. GISAC utilizes HSIN to funnel information to several

sectors and will be expanding that capability for more in future. GISAC also functions as the state's threat management center, meaning that if there is an event going on GISAC will monitor it and send information out to stakeholders as deemed appropriate. This affords GISAC the opportunity to share information with more than law enforcement entities. Thus it provides situational awareness to a broader set of stakeholders that may have a potential interest and/or response to a particular event that is going on within their jurisdiction.

An associated project between the GISAC and state and local law enforcement is the Georgia Terrorism Intelligence Program (GTIP). GTIP is integrated with several metro Atlanta police departments, GBI and GISAC to virtually share, analyze and disseminate terrorism information, generate maps and share/track assets in real time. Seventy percent of the population of Georgia is covered with GTIP (GEMA, n.d.). GTIP allows the sharing of information between agencies, without having to be located in the same physical location, through Web technology, which ensures that all parties have the most up-to-date information possible with which to act upon as appropriate and necessary.

GISAC has made changes to its organizational structure to expand and improve its capabilities over the past eight years. It has only had two directors in this timeframe, which is beneficial from the standpoint of consistency and continuity. The National Governor's Association recognized GISAC as one of three best practices for state level counter-terrorism intelligence centers in 2004. GISAC had a lead role in developing and implementing intelligence operations in support of the 2004 G-8 Summit at Sea Island, Georgia, in collaboration with the U.S. Secret Service, due to its designation as a National Special Security Event. GISAC has been and continues to be involved with special events within the state to provide threat assessments and overall situational awareness about the event for the local, state and federal implications and perspectives. This enhances and increases credibility with partners in the intelligence information-sharing environment.

The legal authority for GISAC's role and function in collecting and analyzing terrorism-related information and conducting follow-up investigations results from

Georgia's Antiterrorism Act, which was passed years before 9/11 to specifically address terrorist threats and illegal acts committed by domestic groups. The Act provides for the development and evaluation of intelligence about persons engaged in terrorist activities, the investigation of acts of terrorism and collaboration with other agencies engaged in counter terrorism activities.

28 CFR Part 23 is the underpinning for all activities in the GISAC. For example, information that may be terrorist related is secured in a "tip file." If a review of the information determines that additional investigation is warranted, officials open a "preliminary file" and begin documenting the use of that information, as required by the regulation. GISAC purges its files every 24 months unless the information is related to an ongoing investigation.

The National Governor's Association, Centers for Best Practice recognized GISAC for their efforts in establishing a fusion center:

Various Georgia state agencies provide personnel for GISAC and the center's analysts and investigators have FBI expertise at their disposal. The single state office, in close proximity to federal agencies, provides fast and coordinated and cross-communication. ...As information is received, it is filtered, documented, and evaluated by analysts. The intelligence product is forwarded to partner agencies, which review it in the context of their particular areas of interest and responsibility. Those agencies may recommend certain actions to disrupt or prevent possible terrorist attacks or to mitigate and manage the consequences of an attack. Agents from GISAC's partners conduct follow-up investigations to determine the credibility, accuracy, and relevancy of current intelligence and to gather additional information. During those investigations, if GISAC agents uncover additional threat intelligence, they alert the appropriate agencies to prevent or disrupt terrorist activity. (National Governor's Association Center for Best Practices [NGA], 2005)

In order to ensure that privacy and civil liberty protections for its citizens were addressed, recognized and adhered to, the GBI Investigation Division developed a "Criminal Intelligence Operations and Privacy Protections" directive in 2008. The purpose of the 17-page directive is "To outline operating procedures and privacy protections for criminal intelligence systems maintained by the Georgia Bureau of Investigation [GBI] and define other operational capabilities of the GBI Intelligence

Unit” (GBI, 2008). The directive states GISAC will comply with the requirements of Title 28, Part 23 of the Code of Federal Regulations, the National Criminal Intelligence Sharing Plan and other relevant federal and state laws regarding criminal intelligence information in Georgia.

The directive clearly defines terms used in the policy, describes how the criminal intelligence system operates; how requests for information are handled; the evaluation and classification of information and the analysis, dissemination, retention and security safeguards of information. The establishment of a Privacy Officer to serve as the security officer is to ensure that information is handled appropriately by providing training, an annual audit and outlines how a user will be dealt with if there is misuse of information within the GISAC. A search conducted on the ACLU of Georgia Web site did not produce any results regarding GISAC, GEMA or GOHS.

A review of the relevant federal guidance for fusion center privacy and civil liberties policy reveals that the GISAC adheres to the “Fair Information Practices,” 28 CFR Part 23. It appears that the ‘issues for consideration’ in the Fusion Center Guidelines document were incorporated, as was the Information Sharing Environment. The Baseline Capabilities guidance was developed after the last revision of the GBI Directive; however, it appears the directive complies with the information outlined in that later guidance.

B. COMMONWEALTH (MASSACHUSETTS) FUSION CENTER

The Massachusetts State Homeland Security Strategy established the Commonwealth Fusion Center (CFC) in October 2004 as the state’s principal center for information collection and dissemination. It was later codified by then Governor Mitt Romney when he signed Executive Order 476 in January 2007. According to the CFC Web site: “The Commonwealth Fusion Center collects and analyzes information from all available sources to produce and disseminate actionable intelligence to stakeholder for strategic and tactical decision-making in order to disrupt domestic and international terrorism” (Commonwealth Fusion Center, n.d.). CFC is an all-threat, all-crime fusion center that encompasses criminal and counter-terrorism analytical support functions.

CFC supports the Massachusetts Emergency Management Agency as necessary in responding to all-hazard incidents that occur within the Commonwealth.

A 2007 GAO report stated:

CFC works with various federal and state and agencies including FBI, ICE, U.S. Coast Guard, HIDTA, Secret Service, TSA, ATF, the United States Marshals Service, U.S. Attorney's Office, the Massachusetts Emergency Management Agency, Massachusetts Department of Fire Services, Department of Public Health, Department of Corrections, and the National Guard. There are 15 analysts assigned to CFC, the majority of who are Massachusetts State Police employees. However, officials said that four of these analysts are assigned to other duties, such as the Crime Reporting Unit or security officer or are otherwise engaged. The Department of Corrections and the Army National Guard have also each assigned an analyst to CFC. All analysts and most sworn members' officers of CFC have Secret clearances, and a few sworn members have Top Secret clearances. The FBI has assigned both an intelligence analyst and special agent to CFC, and DHS has assigned an intelligence officer to the center.

CFC also possesses an investigative component through the Massachusetts State Police Criminal Intelligence Section that provides 5 state troopers and the Massachusetts JTTF, which has 11 state troopers in Boston and Springfield, for a total of 16 investigators assigned to CFC. CFC also has a railroad representative and is involved in public/private outreach through Project Sentinel, which is a program targeting businesses likely to identify precursor terrorist activity. CFC also has personnel assigned to the Boston Regional Intelligence Center, which is the regional intelligence center for the Boston/Cambridge Urban Areas Security Initiative (UASI) region that is led by the Boston Police Department. (pp. 78–79)

The CFC creates four types of intelligence products: bulletins, briefs, report and assessments. It also has a network of various stakeholders that receive these various products based on the classification of the document (unclassified, sensitive but unclassified or law enforcement sensitive) and the stakeholders need-to-know and right-to-know. This affords the CFC the ability to continue its investigation, without compromising it, yet share information to allow other entities to provide it additional information to further that investigation. Depending upon the classification of the product, it could be shared with a wider network of entities thus creating the potential for

information from many sources to aid in their investigation. When CFC produces a bulletin, it is widely distributed to get the information out in a timely manner to alert stakeholders of an imminent event/situation or to provide for their safety. Additionally, it utilizes Geographic Information Systems to enhance products to its customers.

Massachusetts officials reviewed their legislative requirements after 9/11 and conducted a review of existing statutes to determine what laws were applicable to the current counter-terrorism effort and what additional legislation was necessary to protect the public welfare and provide for security against terrorist acts. After that review, the Legislature passed a series of laws that addressed issues associated with the use of hoax substances, the possession of weapons at airports, limitations on public access to sensitive infrastructure data, criminalizing unauthorized possession of explosives and the use/possession of biological and/or chemical weapons and criminalizing the communication of terrorist threats in various media. During the development of the anti-terrorism laws, there was a constant focus on ensuring that basic civil liberties were not weakened within the state.

Since its inception, the ACLU of Massachusetts has consistently challenged the CFCs role and activities. Massachusetts ALCU, Executive Director, Carol Rose stated: “We need a lot more information about what precisely the fusion center will do, what information they will be collecting, who will have access to the information, and what safeguards will be put in place to prevent abuse” (ACLU, 2005). Rose also stated: “The need for transparency and accountability of these centers is paramount ... It is time for Massachusetts to develop public oversight of the Fusion Center, including privacy standards and an annual public evaluation by an independent person or body...” (ALCU MA, 2007).

In 2006, the CFC instituted the “Commonwealth Fusion Center Privacy Policy,” its purpose is “...to ensure safeguards and sanctions are in place to protect personal information as information and intelligence are developed and exchanged. It is the policy of the CFC to protect the legitimate privacy concerns of citizens while conducting its mission.” (Commonwealth Fusion Center [CFC], 2006).

Figure 6 outlines the flow of information handling and evaluation performed at the CFC:

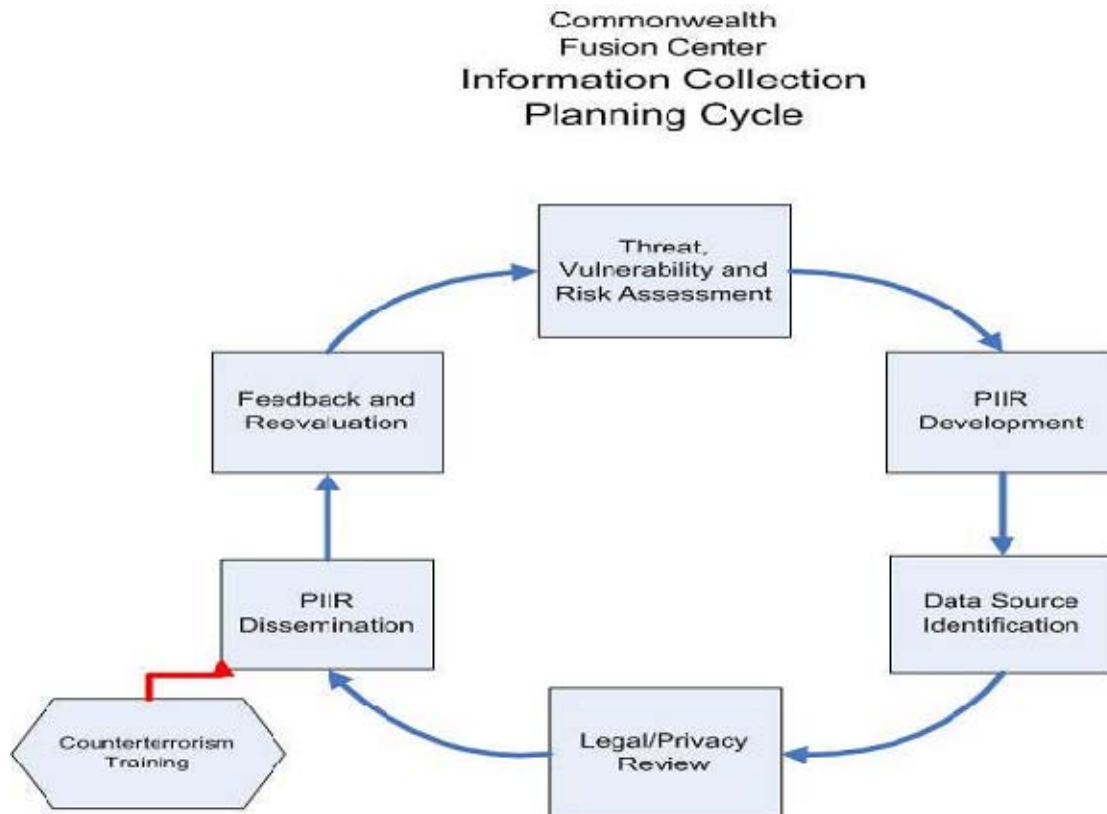


Figure 6. CFC Information Flow (From CFC Operations Manual, 2006)

For clarification purposes on Figure 6, the chart above, PIIR stands for Priority Information/Intelligence Requirements, which are the details of what a customer needs from the intelligence function (CFC, 2006b). The CFC met with stakeholders to discuss various types of information/intelligence they would like to receive. From this, CFC staff members have developed a process to analyze and synthesis that for their customers in terms of the various products CFC creates and distributes.

In reviewing the CFC Privacy Policy, it appears that CFC followed the outline of the “Fusion Center Model Privacy Policy” in Appendix D and adopted the eight privacy design principles of the “Fair Information Practices.” CFC’s policy contains sections on collection limitation, data quality, use limitation, security safeguards, openness, participating agency responsibilities and accountability. It also outlines the

responsibilities of a Compliance Officer who will conduct audits and investigate the misuse of data. References outlined in the policy indicate 28 CFR Part 23 was utilized in the development of the policy.

One area not outlined in the CFC privacy policy is that of an oversight committee which would align them with the ISE Privacy Guidelines – Section 12. However, in the CFC’s “Operations Manual” dated June 2006, it describes the Commonwealth Fusion Center Advisory Council and that it will amongst other things “provide leadership on collection management goals” (CFC, 2006b). It is unclear to this author whether this involves any privacy oversight responsibilities or not. The CFCs 50-page Operations Manual delineates goals, objectives and the operating environment for information sharing and analysis for the state. CFC also developed other SOPs for the center that include, but are not limited to its “National Standards of Intelligence Sharing” and “Processing of Tips and Leads.”

CFC may want to consider producing an annual report on its activities that could be shared with the Legislature, state and local government entities, as well as the Massachusetts ACLU. This would help to reinforce CFC’s goal of protecting privacy and civil liberties while balancing the safety of the citizens of Massachusetts from bad people that may be trying to do bad things within the Commonwealth with less than good intentions.

The Massachusetts Legislature is currently engaged in debate on Senate Bill 931 (SB931) introduced as “An Act Regarding the Commonwealth Fusion Center and Other Intelligence Data Centers” (Chandler, 2009). If passed, it will prohibit law enforcement from collecting information about individuals’ political and religious views, associations or activities, unless it relates directly to a criminal investigation based on reasonable suspicion of criminal conduct. The Bill will create an office of data protection and privacy oversight for all intelligence data centers in Massachusetts. A commissioner who will have full access and subpoena power in order to enable the office to investigate and analyze intelligence data center operations, which includes reports to the public on its findings, will lead this office. The Bill will require basic privacy and quality controls on

data and allow for individuals to access, review and correct information concerning them in order to ensure data accuracy and reliability.

The Massachusetts ACLU fully supports the passage of Senate Bill 931. It surmises that fusion centers collect and compile personal information from an array of public and private electronic sources, operate with very little independent oversight, do not conduct compliance audits and have no quality controls in place. It also believes that SB931 will afford the accountability and oversight that is necessary to protect individual's civil liberty rights and freedoms (American Civil Liberties Union Massachusetts [ACLU MA], 2009).

Carol Rose, Executive Director of ACLU of Massachusetts stated that the CFC "...secretly monitor and collect data on virtually every aspect of our daily lives" and "deploying state and local law enforcement officers as surrogates for federal surveillance efforts" (ACLU MA, 2009). The ACLU's biggest concern is oversight and the fact that other Massachusetts law enforcement agencies were established by statute, yet the CFC was created only by Executive Order (Commonwealth of Massachusetts, 2007). It feels that both the ACLU and the public were left out of the process, which has created anxiety over the activities it perceives are taking place within the CFC. In supporting the passage of SB931, the ACLU feels that Legislative monitoring and the creation of strict standards for data collection, use, accuracy and operational oversight will provide Massachusetts citizens with the protections they inherently deserve.

CFC could perhaps enhance its standing with the ACLU, and others, by providing more transparency in its operations in sharing what it does, how it does what it does and providing documentation of such in a more proactive manner than it has over the past five years. This could be as easy as producing an annual report. In the post 9/11 world, fusion centers need to be seen as credible by advocacy groups, the public as well as by their stakeholders. The more transparent government can be at all levels for ensuring civil liberty protections through such actions as the development of a fully vetted privacy policy, staff trained on privacy issues, procedures and policies and the continued marketing and outreach of fusion centers, the more they will be understood and valued for their mission and purpose—in any state.

Juliette N. Kayyem, Massachusetts Undersecretary for Homeland Security, testified in April 2008 on the first five years of fusion centers and the CFCs progress. She stated:

Just as Hurricane Katrina painfully taught us that a Department solely focused on terrorism may be at risk of undervaluing threats brought by mother nature, a state homeland security apparatus not aligned with the daily need of public safety entities or first responders could not survive or remain relevant. ...The balance at the CFC and in the state we are trying to achieve now has made us reexamine our effort, our policies, and our transparency. ...We will ensure that we will take the proper steps to protect privacy and civil liberties, while continuing to utilize the mechanisms of intelligence and analysis that help protect citizens from critical incidents. (Kayyem, 2008)

Lisa Palmieri, DHS Office of Intelligence and Analysis Intelligence Officer and assigned to the Commonwealth Fusion Center in Massachusetts, stated, “It’s about the flow of information up to the federal government, but also from the government to the state and local level and creates a network to link everyone together and across states” (Stelter, 2009). The growth and refinement of these centers has helped connect agencies, both public and private, across state lines. Palmieri also stated, “We’ve made a lot of progress on information sharing and intelligence sharing” (Stelter, 2009).

C. ARIZONA COUNTER TERRORISM INFORMATION CENTER

The Arizona Counter Terrorism Information Center (AcTIC) was operational in October 2004 as a “cross-jurisdictional partnership among local, state and federal law enforcement; first responders; and emergency management” (GAO, 2007). According to the Arizona Department of Public Safety’s Web site: “The mission of the Arizona Counter Terrorism Information Center is to protect the citizens and critical infrastructures of Arizona by enhancing and coordinating counter terrorism intelligence and other investigative support efforts among local, state and federal law enforcement agencies.” (Arizona Department of Public Safety [AZDPS], 2008).

AcTIC is an all-crimes fusion center that encompasses an investigative, intelligence and analytic support processes for its 24-hour, 7-day a week operation that is

collaboratively managed by the Arizona Department of Homeland Security and the Federal Bureau of Investigation. The center has 24 state, local and federal agencies represented (GAO, 2007).

There are over 200 investigators, analysts and support personnel at the AcTIC, with more than half having Secret clearances. The \$5.3 million dollar, 61,000 square foot facility in north Phoenix, is also home to the Terrorism Liaison Officer (TLO) squad, the HAZMAT/Weapons of Mass Destruction unit, a computer forensics laboratory, the Criminal Investigations Research Unit, Geographical Information Systems and the Violent Criminal Apprehension Program. The facility has workspace for 282 people in two suites. Federal, state and local officials share 157 workstations in one suite while the FBI's Joint Terrorism Task Force and Field Intelligence Group have 125 workstations in an adjacent suite. This affords both groups with the ability to discuss information, cases, tips and such simply by walking to the other's work area. Sharing is predicated upon trust between two (or more) entities and is nurtured through interpersonal communication (NGA, 2005). The co-location of these units is ideal in building the trust between the two main providers and consumers of intelligence information in the AcTIC.

The AcTIC has oversight from two entities: one is a Management Board that consists of the executive from each represented agency; the other is the Governor's Executive Oversight Committee. The oversight committee was created by Executive Order 2005-22, signed by then Governor Napolitano, in 2005. It provides guidance and assurance that the AcTIC operates efficiently and achieves its responsibilities. Arizona also has a Statewide Information Security and Privacy Office, which serves as the strategic planning, facilitation and coordination office for ensuring adequate controls and safeguards are in place for information technology systems and business practices throughout the State. These three entities serve as a check and balance for the AcTIC and are able to recommend changes to the state's Homeland Security Director for changes as deemed appropriate to ensure they meet their mission within the confines of the laws which regulate the AcTIC.

Information/intelligence is received by the AcTICs Watch Center through various sources which is vetted through a series of informational processes before an actionable

intelligence product is released to stakeholders. The dissemination of a product is based upon its security classification and the entities need and right-to-know. Figure 7 illustrates the flow of information through the AcTIC:

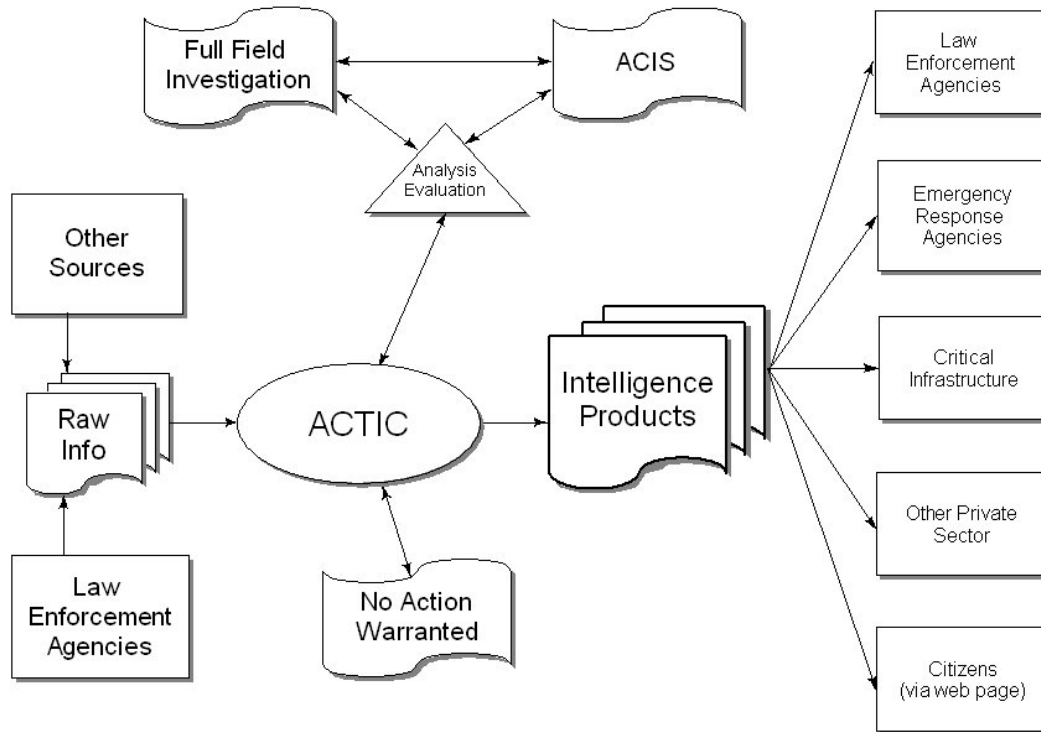


Figure 7. AcTIC Information Flow (From Forsyth, 2005)

In a 2007 GAO report:

AcTIC concentrates on an all-crimes focus for gathering information, which is collected from a variety of Web sites; federal, state, and local databases and networks; the media; and unclassified intelligence bulletins. DHS and DOJ information systems or networks accessible to the center include LEO Special Interest Groups, HSIN-Intel, HSIN-Intel Arizona, and HSDN. AcTIC has direct connectivity to FBI classified systems and networks. However, those AcTIC personnel with Top Secret clearances must enter the JTTF suite and access an FBI system. AcTIC has access to, among others, Regional Information Sharing System (RISS) Automated Trusted Information Exchange (ATIX), SIPRNet, the National Criminal Information Center (NCIC), International Criminal Police Organization (INTERPOL), Financial Crimes Enforcement Network (FinCEN), and El Paso Intelligence Center (EPIC). In total, AcTIC has over 100 law enforcement and public source databases available to it. AcTIC produces biweekly intelligence briefings, advisories, citizens' bulletins, information

collection requirement bulletins, information bulletins, intelligence bulletins, and threat assessments. These products are primarily created for law enforcement entities and specific community partners, but some are for the public (e.g., advisories and citizens' bulletins).

The AcTIC established its Privacy Policy in February 2008 in order to "...provide, in detail, the AcTIC privacy and civil rights protection framework for AcTIC operations" and "...guidance to all AcTIC personnel on the collection, retention and dissemination of criminal information, suspect information and victim information to protect the privacy rights and privileges of Arizona's citizens" (AZDPS, 2008b). The six-page policy outlines the AcTICs governance, oversight and procedures for collection management, data fusion, disclosure, retention and destruction, accountability, enforcement and training. The AcTIC policy incorporated the eight Privacy Design Principles throughout the document as is suggested in DOJ and DHS guidance documents.

The resource list in Appendix A of the DOJ/DHS policy offers a wealth of information that they utilized in the development of their privacy policy. This also allows for easy access and referral to policy-makers and advocates alike to those documents if there are questions. The AcTIC also developed a 27-page "Privacy and Civil Rights Procedure Guide" that outlines procedures for personnel working in the AcTIC to follow well-established policies, procedures, regulations and laws in order to ensure the eight and privacy of Arizona's citizens (AZDPS, 2008a). This document is resource rich and provides employees with significant information as well as training opportunities to further their knowledge in this subject area.

In reviewing the AcTIC privacy policy against federal guidance, it illustrates adherence to the Fusion Center Guidelines, Baseline Capabilities, CFR 28 Part 23 and the ISE. AcTIC is one of the most well regarded of fusion centers in the nation by many in the intelligence community. This is due in part to its transparency and operational diligence in ensuring privacy and civil liberty policies and procedures are adhered to on a daily basis.

D. CONSEQUENCES AND RAMIFICATIONS

The consequences and ramifications for fusion centers that do not focus on privacy and civil liberty issues could be potentially detrimental to the fusion center's existence. Privacy advocates, such as the ACLU and EPIC, government entities, such as the Government Accountability Office and Congressional Research Service, and several news sources have documented fusion centers' exploitation of information and intelligence in methods that are inappropriate and, in some instances, have violated federal and/or state privacy laws and/or statutes. Fusion centers that do not acknowledge, adhere to, or persistently ensure that privacy policies are adhered to, expose themselves to unintentional consequences such as a reduction in capability, over-burdensome oversight, the potential for reduction in funds and resources, a withdrawal of stakeholders, civil lawsuits, loss of credibility, political pressure and the potential shuttering of the center, amongst other possible difficulties.

Centers that do not have a privacy policy, or do not adhere to one, have the potential of being excluded from the larger information-sharing network. The lack of a policy could preclude other states, as well as the federal government, which have privacy policies, from sharing information based on their laws and statutes regarding the information-sharing environment. If a policy does not spell out specific procedures such as, what information the center will collect, how the center protects that information (i.e., 28 CFR Part 23), who has access to the information and such, it could also prevent the sharing of information between entities. For example, a center's policy could state that if another center lacks clearly defined procedures in specific areas (like those aforementioned), then that center will not participate in the information-sharing network with the center that lacks the policy.

Law enforcement investigations rely on protections afforded to them by federal and state laws and statutes, which could include a privacy policy. A privacy policy adds further integrity that data or information will not be shared in-appropriately thus causing

an ongoing investigation to be compromised. Furthermore, most federal agencies will not share or send a representative to a fusion center that does not have a privacy policy; this is for their protection as well.

A center that does not adhere to a privacy policy may be subject to a civil law suit if there is mishandling of personally identifiable information. If a center developed a policy and deviated from that policy by sharing information, the defense will use that deviation in policy against the center in a lawsuit to illustrate injury in the legal sense.

The Federal Privacy Act of 1974 regulates what personal information the federal government can collect about private individuals and how that information can be used. The Privacy Act and the Freedom of Information Act both provide a legal process for accessing personal information. There are exemptions under the both acts that protect information that pertains to national security, criminal investigations or records that might identify an agency's source of confidential information. Although these both have exemptions, fusion centers should not solely rely on them to protect the way they collect, retain and disseminate information.

There are also state laws that pertain to the public accessing information collected by the state on individuals; in New Hampshire, it is RSA 91-A. If a center does not adhere to the 'mission' for which it was created, it exposes itself to possible violations of laws and statutes both at state and federal levels. For example, an all-crime center would not have within its mission to collect information on individuals who may be crossing a state or national border unless it had a criminal predicate to do so; to collect that information on a random basis violates the constitution as well as other possible state and federal laws.

It is important for fusion centers to provide training on privacy and civil liberties for all entities associated with the center on a consistent and constant basis. Personnel need to know how to handle protected individual information responsibly and consistently within applicable laws/statutes, how to identify when privacy incidents occur and how to rectify them. Documentation of training is important to provide for audits and annual reports to demonstrate compliance with privacy policy procedures and federal

guidance on training for center personnel on this topic. If a center cannot provide this type of documentation it further erodes its credibility to ensuring a sound privacy policy is in place and being adhered to. Thus lack of documentation could also be used against it in a civil law suit.

By designating a privacy/compliance officer, fusion centers ensure that there is a dedicated position responsible for coordinating audits and investigating any misuse of data, information and intelligence. There should be a review of all products by this position to identify possible privacy-related concerns before distribution. Without this position, center's risk the possibility that products could be distributed that contain information that is wrong or inappropriate. There have been cases of fusion centers distributing products that included personally identifiable information that was later found to be inaccurate. Consequently, this resulted in the loss of jobs and the center suffering the loss of its credibility with stakeholders, privacy advocates, citizens and the information-sharing environment as a whole which results in over-burdensome oversight for that center.

The consequences and ramifications noted above are not all-inclusive but give a flavor of what some of the possibilities could be for fusion centers that do not fully address and adhere to a privacy policy. A privacy policy protects individual personally identifiable information as well as the disciplines sharing that information.

E. SUMMING IT UP

The three privacy policies reviewed herein are indeed unique to their particular state. The Georgia, Arizona and Massachusetts fusion center officials all seem to follow the myriad of federal guidance to develop a privacy policy in keeping with their center's identified needs. Each fusion center, not just these three, is very different in its focus, governance structure, funding, etc. In addition, each center is subject to its own unique combination of state and federal laws governing intelligence information collection, handling, analysis, dissemination and retention.

In reviewing the CFC's policy, it adhered to the model privacy policy (see Appendix D) which kept its privacy policy short, on point and covered essential elements

described in federal guidance documents that have been presented in this thesis. CFC references are limited to the Fair Information Practices and 28 CFR Part 23.

The AcTIC's privacy policy took a different approach yet covered many of the same basic elements as the CFC's policy. AcTIC officials felt it was important for their policy to include their governance and oversight structure and a small piece on training.

The GISAC privacy policy took yet a different approach than the CFC and AcTIC policies. Its policy was more inclusive of other types of information such as definitions, which enables the reader to know the terms as applied to GISAC.

There are similarities among the three policies: they start out with a purpose statement; they outline applicability and/or accountability; the role of the privacy officer and they all follow the eight privacy design principles (although not the exact wording, except for CFC) as essential functions of their privacy policy. GISAC has a section on training, as does AcTIC; however, CFC's policy does not, other than in the FIP section. AcTIC and GISAC specifically utilize 28 CFR Part 23 in their policy, whereas CFC utilizes it as a reference.

While each of the states' policies differ in structure and form, the underlying concept of the protection of privacy and civil liberties for their citizens is evident by virtue of the existence of a privacy policy. Each state has had to endure varying levels of criticism of its policy, not only from within its own structure and organization but by politicians, legal counsel and privacy advocates who challenge it, sometimes, on a continuous basis.

While challenges are good in a democratic society to ensuring fairness and openness, there also has to be recognition by those challenging the policies that (some) information must be protected to ensure that at every level of government the dots are being connected to prevent bad people from doing bad things in the United States. It is impossible for a privacy policy to conceive of every imaginable situation or set of circumstances that a fusion center may encounter. However, the policy should identify the decision points within the intelligence process and provide guidance and structure for those decision points.

Each entity brings to the fusion center its own functions and resources; however, by coalescing their specialties, they are able to achieve the centers identified mission more economically. Working independently they probably would not come up with same outcome, as there are simply not enough resources available to do the work efficiently and effectively. By utilizing a team approach, it affords the center the opportunity to reduce redundancy, utilize scarce resources in an efficient manner, focus on common objectives and build sustainability and credibility with stakeholders. All disciplines, at all levels of government, need to forget their difficulties and differences to work together. For fusion centers to be truly successful multi-disciplinary partnerships, it is essential that there is a two-way flow of information, both vertically and horizontally. A one-sided approach, by any level of government, will not be successful as was unfortunately discovered on 9/11.

Adherence to established policies and standards will increase the quality of information sharing within the fusion center, with other fusion centers, with the federal intelligence community and the information sharing environment as a whole. The creation and utilization of a national privacy framework would promote a consistent approach to information collection, analysis, dissemination and retention.

The overarching goals of fusion centers are the same—they want to be proactive instead of reactive. It is an overwhelming responsibility, at any level, to identify what information is relevant, when to share it, with whom, under what circumstances, etc. Because of the demand for information and the center's desire for knowledge, the task of synthesizing data into actionable intelligence products needs to happen almost instantaneously. Of the fusion centers that are functional today, the majority fall under the purview law enforcement; however, law enforcement officials have estimated that “approximately 75 percent of the law enforcement agencies in the United States have less than 24 sworn officers, and more often than not, these agencies do not have staff dedicated to intelligence functions” (Global Justice Information Sharing Initiative [Global], 2003, p. iii). A state fusion center can provide law enforcement agencies, as

well as other stakeholders, with vital information to ensure the protection of their citizens—whether it is related to a criminal act, terrorist threat or other hazard that they may encounter within their community.

The concept of ‘boots on the ground’ (firefighters, police officers, EMS, public works, health workers, etc.) armed with validated information from the fusion center, allows a keener sense of awareness where various disciplines, not just law enforcement, are able to make decisions to further investigate areas that might have gone unnoticed in the past. Just as important, this also provides them the ability to provide information/intelligence back to the fusion center to create a bigger picture and possibly connect dots about activities within the community and/or state. For instance, if a fusion center produces an information bulletin on meth labs, and a fire inspector is doing their job and notices items from the bulletin, the inspector can alert law enforcement officials. Or if there is information about sabotage of railroad lines, officials can connect with regulatory and private sector officials to inform them of the situation so they can mitigate the situation as deemed appropriate.

Law enforcement today is not the same as law enforcement 200 years ago, or even 20 years ago. Arguments on the interpretation of laws, guidelines and policies between civil rights advocates and government on these issues will likely continue for the next 200 years. Carter states, “This is why, civil rights issues for fusion centers have components related to policy, training, supervision and public information that must be addressed in the development and implementation stages” (2008, p. 24). If fusion centers focus on ensuring privacy, deal with civil liberty issues with upfront and include a multi-disciplinary committee to review their policies, it would go a long way in building trust with all stakeholders. However, those same stakeholders, citizens and privacy advocates must be cognizant of the fact that they are also the ones that hold the fusion centers responsible for ensuring their safety. If something goes terribly wrong, they will be the ones to lay blame for centers not doing their job. It is a constant balance that is necessary when it comes to information sharing, how much privacy are citizens willing to give up in order to satisfy their need for security.

Civil rights are the rights and freedoms that every citizen possesses as outlined in the U.S. Constitution. A fundamental commitment to protecting civil rights should be the guiding principle in a fusion center's privacy policy. As with any project, there needs to be vision, energy and commitment for it to succeed. Bringing in stakeholders and constituents early on in the development process builds a system of mutual trust and support. There must be commitment and resolve for ensuring sound policies, comprehensive training, effective systems for accountability and supervision are instituted appropriately within fusion centers. It is imperative that if there is a breach of citizen's civil rights that it be acted upon and corrective action taken immediately. This must be done so as not to erode trust and credibility of the center with its stakeholders as well as with advocacy groups.

As noted earlier, the consequences and ramifications are far too reaching for fusion centers to ignore the importance of developing, training on and adhering to a privacy policy.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. RECOMMENDATIONS

When it comes to privacy and accountability, people always demand the former

—David Brin, American science fiction writer

Before making recommendations for developing a privacy policy for the New Hampshire Information and Analysis Center, there are many things to take into consideration:

- What types of information will be collected?
- Who will analyze it?
- Who will develop a product?
- Who decides if there is a product?
- What type of product will it be, is it classified,
- Who is audience?
- Is it urgent, or can it wait?
- Who approves the product?
- What is the dissemination method?
- What governs these?

These and many more decisions that must be made on a daily basis for the fusion center. These are all basic questions that merely skim the tip of the iceberg as far as privacy and civil liberty protections are concerned. There is much thought needed for developing a privacy policy, it requires much more than simply throwing words on paper and announcing its existence—the consequences and ramifications are far to immense.

While information sharing is a controversial topic, it is crucial to ensuring the nation's security. There are federal and state laws that provide protections for citizens from infringement of personal information. A continuous balance must be kept in order

to secure both the privacy and security of U.S. citizens and the nation. Fusion centers can be the underpinnings to that balance if set up with appropriate safeguards, checks and balances and oversight.

The following privacy policy recommendations may provide a forum for discussions at higher levels of government, on the applicability of a national privacy framework that promotes a consistent approach to information collection, analysis, dissemination and retention. The challenge for the federal government, in collaboration with the states, will be how to implement a coordinated approach for privacy policies in consideration of the fact that there are already over 70 fusion centers in various stages of operation (DHS, n.d.).

All levels of government need to clearly understand the importance of institutionalized and systematic protections to privacy and civil liberties for the continued success of fusion centers. How to get there is the topic for another thesis.

A. WHAT IS A PRIVACY POLICY?

The definition of a privacy policy by the U.S. Department of Justice's Privacy and Civil Liberties Policy Development Guide and Implementation Templates:

A privacy policy is a written, published statement that articulates the policy position of an organization on how it handles the personally identifiable information that it gathers and uses in the normal course of business. The policy should include information relating to the processes of information collection, analysis, maintenance, dissemination, and access. The purpose of the privacy policy is to articulate that the agency will adhere to those legal requirements and agency policy determinations that enable gathering and sharing of information to occur in a manner that protects personal privacy interests. A well-developed and –implemented privacy policy uses justice entity resources wisely and effectively; protects the agency, the individual, and the public; and promotes public trust. (Global, 2008b, p. E–7.)

A security policy is different from a privacy policy in that a security policy may not adequately address the protection of personally identifiable information as a privacy policy does. Security policies focus on information classification, protection and a

review process for ensuring information is handled in accordance with the fusion center's privacy policy. Privacy protection is only meaningful if it exists within with a resilient security system.

It is important for fusion centers to develop and implement a privacy policy for the reason succinctly stated in the Privacy Impact Assessment for the Department of Homeland Security State, Local, and Regional Fusion Center Initiative:

A well written privacy policy will force fusion centers to examine and document their legal authorities for undertaking various activities. It will then become the standard to which they train and hold their employees. This will significantly reduce the likelihood that centers will use their powers inconsistent with their authorities. (DHS, 2008, p. 28)

An important facet of the fusion center is to ensure transparency throughout its operation. An annual report and/or a privacy impact assessment—similar to those that DHS compiles—would be a useful tool to provide the center's leadership, stakeholders, privacy advocates and the public with full and open disclosure of the centers activities with regard to privacy and civil liberty issues that it dealt with.

B. PRIVACY BENCHMARKS

In promoting fusion centers achieve a baseline level of capability, the National Strategy for Information Sharing states, "The federal government will support the establishment of these centers and help sustain them through grant funding, technical assistance, and training to achieve a baseline level of capability and to help ensure compliance with all applicable privacy laws" (White House, 2007 p. 20). The strategy outlines specific roles and responsibilities for federal, state, local and tribal authorities in five areas that are related to the establishment and continued operations of fusion centers and for establishing a network of interconnected centers. The areas include:

- General;
- Achieving and sustaining baseline operational standards for state and major urban area fusion centers;
- Suspicious activities and incident reporting;

- Alerts, warnings and notification; and
- Situational awareness reporting.

As the items are addressed in each area, it creates pieces of the governance structure, privacy policy, operational plan and products, amongst other tasks that uniformly relate to all fusion centers. The strategy indicates that the roles and responsibilities were developed in partnership with state and local officials and represent a collective view of the fusion process. While the strategy acknowledges that fusion centers are owned and managed by state and local governments, it identifies the objective is to assist state and local governments in the establishment and sustained operation of these centers. Some fusion center officials have raised concerns at the lack of specificity to-date from the federal government on how it will actually carry out that objective. Most fusion centers do not have the capacity to financially sustain themselves; nor do they have the resources (equipment and personnel) needed to sustain operations without assistance from the federal government. Continued funding, training and technical assistance are essential for sustainability.

Eileen R. Larence, Director, Homeland Security and Justice Issues, stated:

Although fusion centers were primarily established to meet or enhance information sharing within a state or local area, they have become a critical component of the federal government's plans as it works to improve information sharing in accordance with law and policy. Indeed, the National Strategy recognizes fusion centers as vital assets to information sharing and critical in the creation of an integrated national network to promote two-way sharing of terrorism-related information. ...The National Strategy clearly articulates a vision for the federal government's role in supporting centers—that is by helping to sustain centers through grant funding, technical assistance, and training. (GAO, 2008, p. 15.)

The Baseline Capabilities for State and Major Urban Area Fusion Centers, Information Privacy Protections section, outlines five specific areas that fusion centers need to address to ensure a legally sound privacy policy is established:

- Designate a privacy official;
- Develop the privacy policy;

- Address civil liberty and legal rights;
- Conduct outreach and training; and
- Accountability. (DOJ & DHS, 2008)

Appendix A is a spreadsheet that further illustrates the *Information Privacy Protections* in a manner that allows states to document their progress for each of items/tasks in the baseline document. Additionally, the spreadsheet contains a crosswalk to the Target Capabilities List (TCL), National Criminal Intelligence Sharing Plan (NCISP), Fusion Center Guidelines (FCG) and the National Strategy for Information Sharing (NSIS) with the appropriate section/guide to ensure further compliance with federal guidance (DHS, 2007). The TCL describes 37 capabilities related to the four homeland security mission areas of prevent, protect, respond and recover and define and provide the basis for assessing preparedness at all levels of government (DHS, 2007). The NCISP outlines steps that law enforcement agencies at all levels can utilize to ensure that effective intelligence sharing is institutionalized across the law enforcement community. The FCGs ensure centers are established and operated consistently, resulting in enhanced coordination efforts, strengthened partnerships and improved capabilities. The NSIS establishes an integrated information sharing capability to ensure that those who need information will receive it and those who have it will share it.

In many cases, the privacy baseline capabilities exceed the requirements of the ISE Privacy Guidelines, because fusion centers address information types and activities that extend beyond the scope of the ISE (DOJ & DHS, 2008). The ISE is mandated for federal government entities but not state or local governments; however, it makes sense to achieve this higher capability when working with federal entities. Moreover, it further illustrates a state's willingness to further its standards and credibility with its stakeholders.

There have been numerous reports and testimony provided to the federal government on the status and value of fusion centers as a whole, from government officials to advocacy groups and many in between. With respect to establishing a solid foundation for protecting privacy and civil liberties, over the last several years, there have

been numerous forums for discussion at various levels to further collaboration and transparency. In 2006, there were four regional fusion center conferences specifically focused on the importance of a privacy policy. In early 2007, the Fusion Center Privacy Technical Assistance Program was initiated to assist centers to train personnel on privacy policies. In late 2007, four additional regional fusion center meetings took place where fusion center personnel learned the history of privacy and civil liberties in law enforcement intelligence and the importance of developing a privacy policy; this was repeated in 2009 as well. The National Fusion Center Conferences (2007–2009) continue to provide educational sessions on protecting privacy and civil liberties to highlight the importance of these issues and to reinforce the technical assistance sessions offered at the regional conferences. The topic of privacy and civil liberties continues to be an area ripe for discussion and debate as is illustrated throughout this paper.

C. SETTING THE STAGE FOR NEW HAMPSHIRE

What can be leveraged in the analysis of the three privacy policies reviewed in this thesis in creating New Hampshire's IAC privacy policy, realizing an all-threat, all-crime and all-hazard focus? The three fusion center privacy policy's described herein have different origins based upon their particular centers' identified risks, threats, vulnerabilities, laws, statutes, constitution, civil liberty provisions, governance and funding, hence, the differences in the policies. New Hampshire also has different needs, threats, statutes, etc., which will result in a privacy policy that is as diverse as the three reviewed in this thesis.

It is assumed that the following federal guidance documents were utilized to create the basic structure when the centers were established and operationalized:

- National Strategy for Information Sharing;
- Fusion Center Guidelines: Developing and Sharing Information and Intelligence in a New Era;
- Guidelines to Ensure that the Information Privacy and other Legal Rights of Americans are Protected in Development and use of the Information Sharing Environment; and

- National Criminal Intelligence Sharing Plan.

It is also assumed that the *Fusion Center Guidelines* (DOJ & DHS, 2007) list of things to consider when developing a privacy policy were reviewed and incorporated as appropriate. They include:

- Adding introductory language that clearly states the privacy practices of the center.
- Describing the information collected and how information is stored.
- Establishing a common lexicon of terms for dealing with role-based access. Defining and publishing how the information will be used.
- Drafting a clear, prominent and understandable policy.
- Avoid communicating in complicated or technical ways.
- Displaying the privacy policy for both center personnel and customers.
- Ensuring that all other policies and internal controls are consistent with the privacy policy.
- Establishing a business practice of notifying government agencies of suspected inaccurate data.
- Adhering to applicable state and federal constitutional and statutory civil rights provisions.
- Partnering with training centers on privacy protection requirements and conducting periodic privacy security audits.
- Consulting with a privacy committee (see Guideline 3) to ensure that citizens' privacy and civil rights are protected.
- When utilizing commercially available databases, ensuring the usage is for official business and the information obtained is not commingled with private sector data.
- To prevent public records disclosure, risk and vulnerability assessments should not be stored with publicly available data.
- Determining if there are security breach notification laws within the jurisdiction and following those laws, if applicable. (DOJ & DHS, 2007, p. 42)

Building upon this planning base, the following recommendations are provided as guidance in the creation of a succinct and legally sound privacy policy for the NH IAC, or other fusion center at the same point in the process. By utilizing the following recommendations, the policy will address the collection of various types of information, as well as how to compile, blend, analyze and disseminate that information without infringing upon citizens' rights:

- Utilize the “Baseline Capabilities for State and Major Urban Area Fusion Centers, Information Privacy Protections” document (DOJ & DHS, 2008) and specifically the Information Privacy Protections as illustrated in Appendix A of this thesis.
- Utilize the “Privacy and Civil Liberties Policy Development Guide and Implementation Templates” (Global, 2008b). This document incorporates the Fair Information Practices, which are the accepted baseline for privacy protections worldwide.
- Adhere to applicable state and federal constitutional and statutory privacy, civil liberty provisions and right-to-know laws.
- Mandate privacy and civil liberty training programs for IAC personnel.
- Adopt and ensure adherence to 28 CFR Part 23.
- Conduct outreach and provide educational information on the IAC to local, state, federal, private sector, legislative and other entities to ensure a consistent message is conveyed and understood across the spectrum.
- Provide open access to the IAC privacy policy and standard operating guidelines, as allowed under RSA 91-A.
- Establish an IAC advisory committee, to include a cross-section of stakeholders, to review the center's operations and to provide advice regarding security, privacy, data technology, the protection of civil rights and other such matters.
- Conduct an annual meeting with the IAC Advisory Committee, NH Attorney General and representative(s) of a civil liberties organization to report on the operation of the center. This will allow for validation and continued input on how to best ensure the protection of civil rights and personal privacy in a transparent manner.
- Consider developing an audit checklist similar to that of the “Audit Factors for the Law Enforcement Intelligence Function” (Carter. 2008).

- Establish a system to track and resolve privacy complaints, issues or concerns.
- Ensure all fusion center partners comply with all local, state and federal privacy laws.
- Develop a governance structure for the center that includes a cross-section of stakeholders, including law enforcement, public safety, public health, legal, legislative, private sector and federal entities.
 - Establish committees, as necessary, to help execute, adhere to and revise, policies, procedures and programs within the IAC.
 - Oversight Committee—provides review and advice on the center as a whole.
 - Executive Committee—set policy, makes critical decisions and commits resources.
 - Operational Committee—focuses on specific policies, procedures and/or tasks.
 - Technical Committee—focuses on technical standards, critical infrastructure operation and security.
 - Develop by-laws.
 - Utilize parliamentary procedures (i.e., Roberts Rules of Order).
 - Develop memoranda of understanding, non-disclosure agreements and user agreements with partners, as necessary and appropriate.

There does not appear to be a “one size fits all” privacy policy that can be utilized in every state due to differences in state’s laws, statutes, constitution, civil liberty provisions, governance structures, threats, risks, vulnerabilities and funding sources. What works for Massachusetts does not work for Georgia or Arizona and vice versa due to the aforementioned items. For example, the right-to-know laws and/or freedom of information acts are not the same in the three states that are analyzed herein. In New Hampshire, the right-to-know law (RSA 91-A) allows for the release of all information from any department unless it specifically relates to “Records pertaining to matters relating to the preparation for and the carrying out of all emergency functions, including training to carry out such functions, developed by local or state safety officials that are

directly intended to thwart a deliberate act that is intended to result in widespread or severe damage to property or widespread injury or loss of life” (C 91-A:5, 2008a). Each state should take into account its own needs and develop a sound policy that will stand up to legal review, political rhetoric and advocacy challenges.

Outreach and education is necessary and needed to inform state and local government officials, advocacy groups and other stakeholders on what fusion centers are, why they are value-added, to define what products are needed by the various disciplines and how the fusion center can be further leveraged by its constituents. The more fusion centers are discussed and people are exposed to their capabilities, both conceptually and operationally, the more they will be understood and accepted for what they are—a way to connect dots and share information without impinging upon privacy and civil liberties of U.S. citizens.

When developing a privacy policy, a cross-section of various stakeholders should be brought into the process because transparency is crucial and input is essential for building trust—both horizontally and vertically. In New Hampshire, the Department of Safety worked with representatives in drafting legislation to create the IAC. This collaborative process allowed stakeholders the opportunity to provide input and direction to ensure the protection of privacy and civil liberty issues in the state. Ultimately, the legislation did not pass; however, it further strengthened and built consensus and understanding on both sides as to what the issues were and how they could be addressed through the legislative process. It has been suggested that the department utilize (some of the) language from the legislation to create IAC policies and procedures as they have been initially vetted through the legal and legislative process.

There are many federal documents (see Appendix B) that explore policies, resources and organizational issues for states to utilize to develop a privacy policy. Although there is a plethora of information on privacy and civil liberty topics, it is not easy to navigate through the material in a cohesive and efficient manner. Instead of a “one size fits all” privacy policy that clearly does not work, this author would suggest that clear, concise and consistent information be provided. For states to have a single, comprehensive framework to refer to during the development process, instead of

traversing between documents and Web sites, it would save time and provide consistency. In the long run, this type of framework could assist in establishing a nationwide privacy policy program. It is important to note that much has already been developed in terms of privacy documentation by DHS and DOJ for specific purposes for each discipline to include all-crime, all-hazard and counterterrorism. It simply does not make sense from a practical standpoint to have to engage two different federal departments to provide technical assistance in the development of a privacy policy when many components are overlapping and/or necessary, depending upon the type of center a state is developing. Where is the efficiency?

As recommended by the various federal documents, each state should create a privacy policy that follows its constitution, laws and statutes, as well as pertinent federal laws, that are based upon relevant threats and risks. To reiterate, this researcher does not believe, based on the research conducted for this thesis, that there can be a one size fits all privacy policy developed to address each state's individual needs and requirements. However, the development of a single federal framework that contains such items as:

- specific guidance;
- definitions;
- identification of possible issues;
- various templates;
- checklists,

and alike, would assist states in understanding the magnitude of work, thought, collaboration and legal counsel coordination that needs to take place in order to develop their own privacy policy that ensures the protection of citizens civil rights.

THIS PAGE INTENTIONALLY LEFT BLANK

V. CONCLUSION

A free society is a place where it's safe to be unpopular.

—Adlai E. Stevenson, Jr.
(U.S. diplomat and Democratic politician)

The development of a fusion center provides the opportunity to bring together essential resources and produce meaningful information and intelligence for distribution to the right people at the right time for the right reasons. There are many hurdles to overcome in the process of establishing a fusion center privacy policy; however, utilizing the guidance documents developed by the federal government and outlined in this paper is a step in the right direction. Oversight and direction from stakeholders, both inside and outside of government, are essential to the success of the center and should be encouraged.

DOJ and DHS have produced numerous guidance documents to assist states in the development of a privacy policy for their fusion centers. The challenge for the federal government, in collaboration with states, is to put a square peg in a round hole, meaning that there are different governance structures, laws, funding sources, etc. that inhibit each state and that coming up with a “one-size fits all” privacy policy may be near to impossible.

As New Hampshire continues to build-out its capabilities for an Information and Analysis Center, it would be helpful to have one place to go to for technical assistance and guidance on how to create a privacy policy that takes into account all facets of risk, threat and vulnerability. However, it does not seem too likely that will be a possibility in the near future due to the complications of designations of all-crime, counter-terrorism and all-hazard centers, and the fact that these functions are not coordinated by, or even with at times, the same federal departments. There are multiple federal and state agencies that must be involved in order to weave the way through the maze of federal and state laws, regulations, policies and guidance documents. A spreadsheet that clearly illustrates the various pieces to the puzzle would be a good starting point.

As outlined in the case studies between Georgia, Massachusetts and Arizona, their laws and structure simply do not afford any of them the luxury of utilizing the same privacy policy. It is acknowledged that it is vitally important for each state to have a privacy policy and operational procedure in place to govern its fusion center's operations on the collection, analysis and dissemination of intelligence/information to stakeholders. It must also be acknowledged that not every conceivable situation will be able to be represented in the policy. States must also create a policy that outlines redress and the corrective actions that must take place if information is collected and/or disseminated erroneously. The DHS Office of Information and Analysis will respond to states, upon request, to assist in an investigation of misuse of information. This office assists in uncovering what went wrong, at what step of the intelligence process, and help to develop appropriate procedures and processes to correct the problem and ensure that it does not happen again. This can be done through corrective measures such as training and reinforcement of the procedures with all personnel.

All elements of society have an interest in protecting and reducing vulnerability to terrorist attacks. Including government, private sector and the public in a cooperative effort enhances the information sharing process. Accountability, credibility and transparency will be key factors for the success of fusion centers in the future. There needs to be a greater awareness of the value-added that fusion centers bring to the intelligence community whether they are all-crime, counter-terrorism or all-hazard centers (or any combination thereof). They all bring different things to the table based on the state's particular threats, risks and vulnerabilities.

There is only one enemy, the one committed to demolishing this nation, therefore the U.S. must make the protection of the United States and its citizens' way of life its primary mission. Fusion centers are an important piece of the puzzle to ensuring the dots get connected and keeping U.S. citizens safe from all threats—including the rights afforded to them under the United States' Constitution.

APPENDIX A. BASELINE CAPABILITIES—INFORMATION PRIVACY PROTECTIONS

Table 1. Baseline Capabilities (From Department of Homeland Security, Intelligence and Analysis, 2009)

Name:		Title		E-Mail					
Agency:		Telephone Number							
Target Capability	Average Scale Value	Preliminary Capability Finding	Content Expert		Capability Explanation	TCL*	NCISP**	FCG***	N818****
II. Management and Administrative Capabilities		"Fusion centers will have many demands placed on them, and it is important to have clear priorities."—Guideline 2, Fusion Center Guidelines, p. 23, "Establishing a governance structure creates a supported environment that frames the ability for the center to function and operate, assign tasks, allocate and manage resources, and develop and enforce policy."							
B	Information Privacy Protections ¹²								
1	Privacy Official—Fusion centers shall designate an individual to serve as the privacy official and/or establish a privacy committee to be responsible for coordinating the development, implementation, maintenance, and oversight of the privacy protection policies and procedures. (ISE Privacy Guidelines—Section 12)							Guideline 8	ISE Privacy Guidelines Section 12
				1a	If the privacy official is not an attorney, the fusion center shall have access to legal counsel to help clarify laws, rules, regulations, and statutes governing the collection, maintenance, and dissemination of information and assist with the development of policies, procedures, guidelines, and operation manuals.				
				1b	The privacy official or committee should review all other fusion center policies and procedures to ensure consistency with the privacy policy.				
				1c	The privacy official or committee shall coordinate with the center's designated security officer to ensure that security measures provide the proper protection to information in compliance with all applicable laws and the center's privacy policy protection policies.				
				1d	Identify stakeholders to include nongovernment organizations, advocates, the media, and others that are essential to the development and implementation of the privacy policy.				
				1d(i)	To the extent possible, fusion centers should use existing outreach mechanisms, such as a state or local government's privacy advisory committee, or outreach conducted by the state or local law enforcement or homeland security organizations to facilitate engagement with the community and privacy advocacy groups.				
2	Privacy Policy Development—in developing the privacy policy, fusion centers shall:			2a	Develop guidance statements that include the vision, mission, values statements, goals, and objectives for the creation of the privacy policy. (ISE Privacy Guidelines—Section 3)				
				2b	Develop a project charter that will include an introduction, background, membership, and the previously drafted guidance statements.				
				2c	Analyze the flow of information and the legal environment for the protection of privacy to identify what gaps exist between existing technological and legal requirements.				
				2c(i)	Information flow analysis helps determine what personally identifiable information the agency collects, uses, maintains, and disseminates. (ISE Privacy Guidelines—Section 4)				
				2c(i)(a)	Identify the fusion centers data holdings and establish mechanisms to ensure their review before protected information is shared through the ISE.				

Target Capability		Average Scale Value	Preliminary Capability Finding	Content Expert	Capability Explanation	TCL*	NCISF**	FCG***	N318****
					2c(i)(b) Establish mechanisms to identify the nature of protected information so it can be handled in accordance with applicable legal requirements.				
					2c(ii) All policies and procedures are compliant with the U.S. Constitution, the state's constitution, applicable laws, and executive orders. (ISE Privacy Guidelines--Section 2)				
					2c(ii)(a) Conduct a rules assessment and adopt policies and procedures requiring the fusion center to seek, receive, or retain only the protected information which it is legally permitted to seek, receive, or retain and which was lawfully obtained.				
					2c(ii)(b) Establish a process to allow for the ongoing identification and assessment of new and/or revised laws, court decisions, and policies that impact issues related to privacy, civil rights, and civil liberties.				
					2c(ii)(c) If an issue posing a significant risk to privacy is identified, develop policy and procedural protections.				
					2d Perform a gap analysis to identify legal and technological gaps.				
					2e Vet the privacy protection policy internally and externally during its development by soliciting commentary and buy-in from stakeholders and agency constituents prior to finalizing the policy.	ComG 1.4	Recommendation 6	Guideline 8	ISE Privacy Guidelines - Section 3 & 12.d
					2f Formally adopt a privacy protection policy to guide the collection, use, maintenance, and dissemination of personal information. (ISE Privacy Guidelines--Section 12.d.)				
					2f(i) Obtain formal adoption of the policy by the project team, privacy and civil liberties officer, the fusion center's governance structure and, if applicable, any legislative body.				
3	Privacy Protections--Fusion centers shall develop and implement a privacy protection policy that ensures that the center's activities (collection/gathering, analysis, dissemination, storage, and use of information) are conducted in a manner that protects the privacy, civil liberties, and other legal rights of individuals protected by applicable law, while ensuring the security of the information shared. The policy shall cover all center activities and shall be at least as comprehensive as the requirements set forth in the Information Sharing Environment Privacy Guidelines and consistent with 28 CFR Part 23 and DOJ's Global Privacy and Civil Liberties Policy Development Guide and Implementation Templates.					ComG 1.2.1 & 3.1.2; Pre-A1c 3.6	Recommendations 9 & 15	Guideline 8	
					3a The privacy protection policy shall include procedures to ensure data quality. (ISE Privacy Guidelines--Section 5)				
					3a(i) Establish accuracy procedures to ensure that information is accurate, and prevent, identify, and correct errors regarding (1) protected information and (2) any erroneous sharing of information in the ISE.				
					3a(ii) Establish and implement a process to provide written error notice of any potential error or deficiency to the privacy official of the source agency when it is determined that the protected information received may be erroneous, includes incorrectly merged information, or lacks adequate context such that the rights of the individual may be affected.				
					3a(iii) Adopt and implement the ISE policies and procedures for merger of information, investigation, and correction/deletion/in-use of erroneous or deficient information, and retain only information that is relevant and timely for its appropriate use.				
					3b Establish criteria for types of information that partners can submit to the center.				
					3c Include provisions for the use of privately held data systems information and commercially obtained data.				
					3d Review the center's security policies and ensure that they are sufficient for providing appropriate physical, technical, and administrative measures to safeguard protected information. (See Section II.C. and ISE Privacy Guidelines--Section 5.)				
					3d(i) Ensure that the center's privacy and civil liberties policy articulates a process for responding to and addressing security breaches, in coordination with the center's designated security officer. (See Section II.C.2.)				

Target Capability		Average Scale Value	Preliminary Capability Finding	Content Expert	Capability Explanation	TCL*	NCISP**	FCG***	N318****
				3e	The privacy protection policy shall include documentation on how the policies and procedures meet the following ISE Privacy Guidelines requirements (ISE Privacy Guidelines--Section 12):				
				3e(i)	Fusion centers shall adopt policies and procedures limiting the sharing of information through the ISE to terrorism, homeland security, and law enforcement (terrorism-related) information, as defined for the ISE (see Glossary) and ensure that access to and use of protected information ²³ are consistent with the authorized purpose of the ISE. ²⁴ (ISE Privacy Guidelines--Section 3)				
				3e(ii)	Fusion centers shall identify protected information to be shared through the ISE.				
4	Privacy Policy Outreach--Fusion centers shall implement necessary outreach and training for the execution, training, and technology aspects of the privacy protection policy. (ISE Privacy Guidelines--Section 9)							Guideline 8	ISE Privacy Guidelines Section 9
				4a	Ensure that privacy protections are implemented through training, business process changes, and system designs.				
				4b	Provide ongoing training to center personnel and any other liaison partners on the fusion center's privacy policies and procedures. Training should be tailored to the audience (management, analysts, collectors, consumers of center products, etc.) but, at a minimum, should include:				
				4b(i)	An overview of the policies and procedures for collection, use, disclosure of protected information, data quality, accountability, enforcement, auditing, and redress.				
				4b(ii)	How to report violations of the privacy policy.				
				4b(iii)	An overview of sanctions or enforcement mechanisms for failure to comply with the privacy policy.				
				4c	Consider and implement appropriate privacy-enhancing technologies.				
				4d	Fusion centers shall facilitate public awareness of their privacy protection policy by making it available to the public or otherwise facilitating appropriate public awareness. (ISE Privacy Guidelines--Section 10)				
						ComG 3.1.3		Guideline 8	ISE Privacy Guidelines Section 7
				5a	Fusion centers shall develop or modify policies, procedures, and mechanisms for accountability, enforcement, and auditing of the center's privacy protection. (ISE Privacy Guidelines--Section 7)				
				5a(i)	Require reporting, investigating, and responding to violations of the center's privacy protection policy.				
6	Privacy Policy Accountability--Fusion centers shall ensure accountability with regard to the privacy protection policy and identify evaluation methods for auditing and monitoring the implementation of the privacy policy and processes to permit individual redress and incorporate revisions and updates identified through the evaluation and monitoring as well as redress processes. (ISE Privacy Guidelines--Section 7)			5a(ii)	Encourage cooperation with audits and reviews.				
				5a(iii)	Provide for receipt of error reports by the agency privacy official or committee. (See Section B.2., above.)				
				5a(iv)	Implement adequate review and audit mechanisms to verify the center's compliance with its privacy protection policy.				
				5a(v)	Incorporate the core elements of the ISE Privacy Guidelines' Accountability, Enforcement, and Audit guidance into the fusion center ISE privacy policy.				
				5b	Fusion centers shall develop internal procedures for redress--particularly to address complaints from protected persons regarding personally identifiable information about them under fusion center control. (ISE Privacy Guidelines--Section 8)				
				5b(i)	Incorporate the core elements of the ISE Privacy Guidelines Redress guidance into the fusion center ISE privacy protection policy.				

Target Capability		Average Scale Value	Preliminary Capability Finding	Content Expert		Capability Explanation	TCL*	NCISF**	FCG***	NSIS****
					Sc	Fusion centers should utilize the LEIU Audit Checklist for the Criminal Intelligence Function when reviewing their "criminal intelligence function to demonstrate their commitment to protecting the constitutional rights and the privacy of individuals, while ensuring the operational effectiveness of their criminal intelligence function." ²⁵				
22	These capabilities were developed to ensure that the privacy policies that fusion centers adopt are at least as comprehensive as the IBE Privacy Guidelines (see the Methodology section for further background). The achievement of these capabilities will result in a fusion center privacy protection policy that meets the IBE Section 12.d requirement of the IBE Privacy Guidelines.									
23	The term "protected information" is defined in the IBE Privacy Guidelines, Section 1.b., for both non-intelligence agencies and members of the Intelligence Community. For both federal non-intelligence agencies and SLT agencies, it means, at a minimum, personally identifiable information about U.S. citizens and lawful permanent residents. State are free to extend this definition to other classes of persons or to all persons (including organizations).									
24	The authorized purpose of the IBE is to share terrorism-related information in a lawful manner that protects the privacy and other legal rights of Americans between and among authorized recipients of such information. (IBE Privacy Guidelines-Section 3)									
25	LEIU Audit Checklist for the Criminal Intelligence Function, p.i.									
TCL*		Target Capability List								
NCISF**		National Criminal Intelligence Sharing Plan								
FCG***		Fusion Center Guidelines								
NSIS****		National Strategy for Information Sharing								

APPENDIX B. RESOURCES FOR PRIVACY POLICY DEVELOPMENT

Audit Checklist. This checklist was developed by the Law Enforcement Intelligence Unit (LEIU), in support of the National Criminal Intelligence Sharing Plan. This is a tool that can be utilized to conduct an audit/evaluation of an agency's criminal intelligence function.

U.S. Department of Justice. (2004). *Audit Checklist for the Criminal Intelligence Function*. Washington, DC: author. Retrieved December 6, 2009, from http://it.ojp.gov/documents/LEIU_audit_checklist.pdf

Baseline Capabilities for State and Major Urban Area Fusion Centers. Developed by the U.S. Department of Justice and U.S. Department of Homeland Security provides a section specifically on information privacy protections in a detailed format.

U.S. Department of Justice and U.S. Department of Homeland Security (2008). *Baseline Capabilities for State and Major Urban Area Fusion Centers A Supplement to the Fusion Center Guidelines*. Washington, DC: authors. Retrieved December 6, 2009, from <http://it.ojp.gov/documents/baselinecapabilitiesa.pdf>

Fusion Center Guidelines Developing and Sharing Information and Intelligence in a New Era. Developed by the U.S. Department of Justice and U.S. Department of Homeland Security. Guideline 8 is dedicated to privacy and civil liberties.

U.S. Department of Justice and U.S. Department of Homeland Security. (2006). *Fusion Center Guidelines Developing and Sharing Information and Intelligence in a New Era*. Washington, DC: authors. Retrieved December 6, 2009, from http://it.ojp.gov/documents/fusion_center_guidelines_law_enforcement.pdf

Justice Information Privacy Guideline. Developed by the National Criminal Justice Association this document provides guidance on public safety, public access and privacy for the development of information privacy policies.

National Criminal Justice Association. (2002, September) *Justice Information Privacy Guide*. Washington, DC: author. Retrieved December 6, 2009, from <http://www.ncja.org/Content/NavigationMenu/PoliciesPractices/JusticeInformationPrivacyGuideline/privacyguideline.pdf>

National Criminal Intelligence Sharing Plan. Developed by the U.S. Department of Justice's (DOJ) Global Justice Information Sharing Initiative (Global) provides a series of recommendations for privacy policy development.

Global Justice Information Sharing Initiative, Office of Justice Programs, U.S. Department of Justice. (2003). *National Criminal Intelligence Sharing Plan*. Washington, DC: Department of Justice. Retrieved December 6, 2009, from http://it.ojp.gov/documents/National_Criminal_Intelligence_Sharing_Plan.pdf

Privacy, Civil Rights, and Civil Liberties Policy Templates for Justice Information Systems. Developed by the U.S. Department of Justice's (DOJ) Global Justice Information Sharing Initiative this document provides templates for drafting comprehensive policies to protect privacy, civil rights, and civil liberties principles.

Global Justice Information Sharing Initiative, Office of Justice Programs, U.S. Department of Justice. (2008, February). *Privacy, Civil Rights, and Civil Liberties Policy Templates for Justice Information Systems*. Washington, D.C. Retrieved December 6, 2009, from http://it.ojp.gov/documents/Privacy_Civil_Rights_and_Civil_Liberties_Policy_Templates.pdf

Privacy and Civil Liberties Policy Development Guide and Implementation Templates. Developed by the U.S. Department of Justice's (DOJ) Global Justice Information Sharing Initiative (Global), provides information on developing and implementing privacy policies.

Global Justice Information Sharing Initiative, Office of Justice Programs, U.S. Department of Justice. (2008, February). *Privacy and Civil Liberties Policy Development Guide and Implementation Templates*. Washington, DC: department of Justice. Retrieved December 6, 2009, from http://it.ojp.gov/privacy206/privacy_policy_development_guide.pdf

Privacy and Information Quality Policy Development for the Justice Maker. Developed by U.S. Department of Justice's Global Justice Information Sharing Initiative. The document is a quick guide to privacy and information quality policies.

Global Justice Information Sharing Initiative, Office of Justice Programs, U.S. Department of Justice. (2008). *Privacy and Information Quality Policy Development for the Justice Maker*. Washington, DC: Department of Justice. Retrieved December 6, 2009, from http://it.ojp.gov/documents/global_privacy_brief.pdf

28 CFR Part 23. U.S. Department of Justice. This is the national standard for sharing criminal intelligence information to ensure that criminal intelligence systems conform with the privacy and constitutional rights of individuals.

U.S. Department of Justice. (2001). *Code of Federal Regulations, Title 28--Judicial Administration, Chapter I--Department of Justice, Part 23--Criminal Intelligence Systems Operating Policies*. Washington, D.C. Retrieved December 6, 2009, from http://www.access.gpo.gov/nara/cfr/waisidx_01/28cfr23_01.html

APPENDIX C. COMPENDIUM OF NEW HAMPSHIRE'S PRIVACY AND SECURITY LEGISLATION

Table 2. Compendium of New Hampshire's Privacy and Security Legislation (From Bureau of Justice Statistics, 2003, pp. 114–115)

	Category	Citation
1	State Regulatory Authority	106-B:14
2	Privacy and Security Council	Reg. 7.C, D
3	Dissemination Regulations	
	Conviction Information	
3.10	Authorizes to Criminal Justice Agencies	Reg. 3.B.2; Gen. 106-B:14, :14-a; 651-B:7
3.11	Authorizes to Govt. Noncriminal Justice Agencies	170-E:7, -G:8-c; 189:13-a; 328-B:4; Reg. 3.B
3.12	Authorizes to Private Sector	159-C:2; Reg. 3.B
3.13	Prohibits to Criminal Justice Agencies	159-C:3
3.14	Prohibits to Govt. Noncriminal Justice Agencies	159-C:3
3.15	Prohibits to Private Sector	159-C:3
	Nonconviction Information	
3.20	Authorizes to Criminal Justice Agencies	Reg. 3.A.2
3.21	Authorizes to Govt. Noncriminal Justice Agencies	Reg. 3.B.8
3.22	Authorizes to Private Sector	Reg. 3.B.8
3.23	Prohibits to Criminal Justice Agencies	
3.24	Prohibits to Govt. Noncriminal Justice Agencies	Reg. 3.B.3
3.25	Prohibits to Private Sector	Reg. 3.B.3
	Arrest Information	
3.30	Authorizes to Criminal Justice Agencies	Reg. 3.A.2
3.31	Authorizes to Govt. Noncriminal Justice Agencies	Reg. 3.B.8
3.32	Authorizes to Private Sector	Reg. 3.B.8
3.33	Prohibits to Criminal Justice Agencies	
3.34	Prohibits to Govt. Noncriminal Justice Agencies	Reg. 3.B.3
3.35	Prohibits to Private Sector	Reg. 3.B.3
4	Inspection	
4.1	Right to Inspect Only	
4.2	Right to Inspect and Take Notes	
4.3	Right to Inspect and Obtain Copy	91-A:4; Reg. 3.B.9
5	Right to Challenge	Reg. 7
6	Judicial Review of Challenged Information	
7	Purging Nonconviction Information	Reg. 3.D
8	Purging Conviction Information	651:5; Reg. 3.D
9	Sealing Nonconviction Information	
10	Sealing Conviction Information	318-B:28-a; 651:5
11	Removal of Disqualifications	651:5; Reg. 3.D
12	Right to State Nonexistence of Record	651:05:00

	Category	Citation
13	Research Access	Reg. 3.B.7
14	Accuracy and Completeness	
14.1	Disposition Reporting Requirements	106-B:14, 14-a
14.2	Auditing Requirements	Reg. 5
14.3	Other Accuracy/Completeness Requirements	Reg. 4
15	Dedication	
16	Civil Remedies	
17	Criminal Penalties	106-B:14; 159-C:10; 651:5.X
18	Public Records	7-A:1; 91-A:4
19	Separation of Files	
20	Regulation of Intelligence Collection	
21	Regulation of Intelligence Dissemination	
22	Security	
22.1	Physical (Building) Security	Reg. 1
22.2	Administrative Security	Reg. 2
22.3	Computer Security	
23	Transaction Logs	Reg. 3.C.4
24	Training Employees	
25	Listing of Information Systems	7-A:2
26	FOIA (Including CJI)	
27	FOIA (Excluding CJI)	91-A:5; 106-B:14
28	Central State Repository	106-B:14
29	National Crime Prevention and Privacy Compact Enacted	
	<p>This Compendium is the latest in a series of 12 U.S. Department of Justice publications that reference and analyze State laws and regulations relating to privacy and security of criminal history record information. These compendia include: (1) compilations of State laws and administrative regulations, and (2) analyses of findings and trends reflected in that body of law and policy documents. The purpose of these compendia is to assist legislators, planners, administrators, legal analysts and others interested in reviewing State statutes and regulations governing the maintenance and use of criminal records, and in analyzing national trends in this important area. Comparing and contrasting the various approaches reflected in the many State laws and regulations cited in these documents should assist planners and administrators in developing effective and fair policies for their jurisdictions. By facilitating such comparisons and by furthering research in this area, the compendia are intended to promote the evolution of enlightened privacy and information policy. (Compendium of State Security and Privacy Legislation: Overview 2002. 2003, November).</p>	

APPENDIX D. FUSION CENTER MODEL PRIVACY POLICY SAMPLE TEMPLATE (FROM FUSION CENTER MODEL, 2004)

*This document should only be used as a sample. The user is encouraged to add
And delete items contained within this sample document as appropriate.*

Fusion Center Model Privacy Policy

I. Purpose

The _____ is a Fusion Center
(herein referenced to as “Center”) as defined below:

*A Fusion Center is a collaborative effort of two of more agencies who
provide resources, expertise, and/or information to the Center with the
goal of maximizing the ability to detect, prevent, apprehend, and respond
to criminal and terrorism activity.*

The Fusion Center project was initiated in response to the increased need for timely information sharing and exchange of crime-related information among members of the law enforcement community. One component of the Center focuses on the development and exchange of criminal intelligence. This component focuses on the intelligence process where information is collected, integrated, evaluated, analyzed and disseminated.

The Center’s intelligence products and services will be made available to law enforcement agencies and other criminal justice entities. All agencies participating in the Center will be subject to a Memorandum of Understanding and will be required to adhere to all Center policies and security requirements. The purpose of this privacy policy is to ensure safeguards and sanctions are in place to protect personal information as information and intelligence are developed and exchanged.

This *Privacy Policy* embraces the eight Privacy Design Principles developed by the Organization of Economic Cooperation and Development’s *Fair Information Practices* and shall be used to guide the policy wherever applicable. The eight Privacy Design Principles are:

1. **Purpose Specification**—Define agency purposes for information to help ensure agency uses of information are appropriate.
2. **Collection Limitation**—Limit the collection of personal information to that required for the purposes intended.
3. **Data Quality**—Ensure data accuracy.
4. **Use Limitation**—Ensure appropriate limits on agency use of personal information.

5. **Security Safeguards**—Maintain effective security over personal information.
6. **Openness**—Promote a general policy of openness about agency practices and policies regarding personal information.
7. **Individual Participation**—Allow individuals reasonable access and opportunity to correct errors in their personal information held by the agency.
8. **Accountability**—Identify, train, and hold agency personnel accountable for adhering to agency information quality and privacy policies.

The Center has developed databases by using existing data sources from participating entities to integrate data with the goal of identifying, developing, and analyzing information and intelligence related to terrorist activity and other crimes for investigative leads. This capability will facilitate integration and exchange of information between the participating agencies.

II. Collection Limitation

The Center is maintained for the purpose of developing information and intelligence by agencies participating in the project. The decision of the agencies to participate in the Center and about which databases to provide is voluntary and will be governed by the laws and rules governing the individual agencies respecting such data, as well as by applicable federal laws.

Because the laws, rules, or policies governing information and intelligence that can be collected and released on private individuals will vary from agency to agency, limitations on the collection of data concerning individuals is the responsibility of the collector of the original source data. Each contributor of information is to abide by the collection limitations applicable to it by reason of law, rule, or policy. Information contributed to the Center should be that which has been collected in conformance with those limitations.

III. Data Quality

The agencies participating in the Center remain the owners of the data contributed and are, therefore, responsible for the quality and accuracy of the data accessed by the Center. Inaccurate personal information can have a damaging impact on the person concerned and on the integrity and functional value of the Center. In order to maintain the integrity of the Center, any information obtained through the Center must be independently verified with the original source from which the data was extrapolated *before* any official action (e.g., warrant or arrest) is taken. User agencies and individual users are responsible for compliance with respect to use and further dissemination of such information and the purging and updating of the data.

IV. Use Limitation

Information obtained from or through the Center can only be used for lawful purposes. A lawful purpose means the request for data can be directly linked to a law enforcement agency's active criminal investigation or is a response to a confirmed lead that requires follow-up to prevent a criminal act.

The Governance Board of the Fusion Center will take necessary measures to make certain that access to the Center's information and intelligence resources is secure and will prevent any unauthorized access or use. The Board reserves the right to restrict the qualifications and number of personnel who will be accessing the Center and to suspend or withhold service to any individual violating this *Privacy Policy*. The Board, or persons acting on behalf of the Board, further reserves the right to conduct inspections concerning the proper use and security of the information received from the Center.

Security for information derived from the Center will be provided in accordance with applicable laws, rules, and regulations. Furthermore, all personnel who receive, handle, or have access to Center data and/or sensitive information will be trained as to those requirements. All personnel having access to the Center's data agree to abide by the following rules:

1. The Center's data will be used only to perform official law enforcement investigative-related duties in a manner authorized by the user's employer.
2. Individual passwords will not be disclosed to any other person except as authorized by agency management.
3. Individual passwords will be changed if authorized personnel of the agency or members of the Center suspect the password has been improperly disclosed or otherwise compromised.
4. Background checks will be completed on personnel who will have direct access to the Center.
5. Use of the Center's data in an unauthorized or illegal manner will subject the user to denial of further use of the Center, discipline by the user's employing agency, and/or criminal prosecution.

Each authorized user understands that access to the Center can be denied or rescinded for failure to comply with the applicable restrictions and use limitations.

V. Security Safeguards

Information obtained from or through the Center will not be used or publicly disclosed for purposes other than those specified in the Memorandum of Understanding that each participating agency must sign. Information cannot be (1) sold, published, exchanged, or disclosed for commercial purposes; (2) disclosed or published without prior approval of the contributing agency; or (3) disseminated to unauthorized persons.

Use of the Center's data is limited to those individuals who have been selected, approved, and trained accordingly. Access to information contained within the Center will be granted only to law enforcement agency personnel who have been screened with a state and national fingerprint-based background check, as well as any additional background screening processes using procedures and standards established by the Fusion Center Governance Board. Each individual user must complete an Individual User Agreement in conjunction with training.

Access to the Center's databases from outside of the Center will only be allowed over secure network lines.

VI. Openness

It is the intent of the participating agencies to be open with the public concerning data collection practices when such openness will not jeopardize ongoing criminal investigative activities. Participating agencies will refer citizens to the original collector of the data as the appropriate entity to address any concern about data accuracy and quality, when this can be done without compromising an active inquiry or investigation.

All agencies participating in the Center will make this *Privacy Policy* available for public review. The Center will post this *Privacy Policy* on its public Web site and make it available to any interested party.

VII. Individual Participation

The data maintained by the Center is provided, on a voluntary basis, by the participating agencies or is information obtained from other sources by the Center. Each individual user searching against the data as described herein will be required to acknowledge that he or she remains solely responsible for the interpretation, further dissemination, and use of any information that results from the search process and is responsible for ensuring that any information relied upon is accurate, current, valid, and complete, especially before any official action is taken in full or partial reliance upon the information obtained.

Members of the public cannot access individually identifiable information, on themselves or others, from the Center's applications. Persons wishing to access data pertaining to themselves should communicate directly with the agency or entity that is the source of the data in question.

Participating agencies agree that they will refer requests related to privacy or sunshine laws back to the originator of the information.

VIII. Accountability

When a query is made to any of the Center's data applications, the original request is automatically logged by the system identifying the user initiating the query. When such information is disseminated outside of the agency from which the original request is made, a secondary dissemination log must be maintained in order to correct possible erroneous information and for audit purposes, as required by applicable law. Secondary dissemination of information can only be to a law enforcement agency for a law enforcement investigative purpose or to other agencies as provided by law. The agency *from* which the information is requested will maintain a record (log) of any secondary dissemination of information. This record will reflect as a minimum:

1. Date of release.
2. To whom the information relates.
3. To whom the information was released (including address and telephone number).
4. An identification number or other indicator that clearly identifies the data released.
5. The purpose for which the information was requested.

The Governance Board will be responsible for conducting or coordinating audits and investigating misuse of the Center's data or information. All violations and/or exceptions shall be reported to the Board. Individual users of the Center's information remain responsible for their legal and appropriate use of the information contained therein. Failure to abide by the restrictions and use limitations for the use of the Center's data may result in the suspension or termination of use privileges, discipline sanctions imposed by the user's employing agency, or criminal prosecution. Each user and participating agency in the Center is required to abide by this *Privacy Policy* in the use of information obtained by and through the Center.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX E. DEFINITIONS FOR PRIVACY POLICY DEVELOPMENT

The following definitions are provided from several sources to provide context and continuity for this thesis.

The following definitions are provided from New Hampshire Revised Statutes Annotated (RSA) 91-A:1-a:

1. *Governmental records* means any information created, accepted, or obtained by, or on behalf of, any public body, or a quorum or majority thereof, or any public agency in furtherance of its official function. Without limiting the foregoing, the term “governmental records” includes any written communication or other information, whether in paper, electronic, or other physical form, received by a quorum or majority of a public body in furtherance of its official function, whether at a meeting or outside a meeting of the body. The term ‘governmental records’ shall also include the term ‘public records.’” (NHRSA, 2008c)
2. *Information* means knowledge, opinions, facts, or data of any kind and in whatever physical form kept or maintained, including, but not limited to, written, aural, visual, electronic, or other physical form. (NHRSA, 2008c).
3. *Public agency* means any agency, authority, department, or office of the state or of any county, town, municipal corporation, school district, school administrative unit, chartered public school, or other political subdivision. (NHRSA, 2008c).

The following definitions are provided from the National Criminal Intelligence Sharing Plan:

1. ...the term *constitutional rights* refers to those rights that an individual derives from the Constitution of the United States. Constitutional rights are the strongest protection from improper government conduct against an individual. Unlike other legal rights, constitutional rights cannot be changed by a statute. They can only be altered by amending the Constitution. (Global, 2003, p. 5)
2. The term *civil liberties* refers to fundamental individual rights such as freedom of speech, press, or religion; due process of law; and other limitations on the power of the government to restrain or dictate the actions of individuals. They are the freedoms that are guaranteed by the Bill of Rights—the first ten Amendments—to the Constitution of the

United States. Civil liberties offer protection to individuals from improper government action and arbitrary governmental interference in relation to the specific freedoms enumerated in the Bill of Rights. (Global, 2003, p. 5)

3. The term *civil rights* is used to imply that the state has a role in ensuring all citizens have equal protection under the law and equal opportunity to exercise the privileges of citizenship regardless of race, religion, sex, or other characteristics unrelated to the worth of the individual. Civil rights are, therefore, obligations imposed upon government to promote equality. More specifically, they are the rights to personal liberty guaranteed to all United States citizens by the Thirteenth and Fourteenth Amendments and by acts of Congress. Generally, the term *civil rights* involves positive (or affirmative) government action, while the term *civil liberties* involves restrictions on government. (Global, 2003, pp. 5–6)
4. The term *privacy* refers to individuals' interests in preventing the inappropriate collection, use, and release of personally identifiable information. Privacy interests include privacy of personal behavior, privacy of personal communications, and privacy of personal data. The U.S. Constitution does not explicitly use the word *privacy*, but several of its provisions protect different aspects of this fundamental right. Although there does not exist an explicit federal constitutional right to an individual's privacy, privacy rights have been articulated in limited contexts by the U.S. Supreme Court. (Global, 2003, p. 6)
5. The protection of individuals' privacy and constitutional rights is an obligation of government officials and is crucial to the long-term success of criminal intelligence sharing. Protecting the privacy and constitutional rights of individuals, while at the same time providing for homeland security and public safety, will require a commitment from everyone in the system—from line officers to top management. (Global, 2003, p.5)

The following definitions are provided from New Hampshire House Bill 587:

1. *Criminal intelligence information* means information and data that have been determined through evaluation to be relevant to the identification of actual and impending criminal activity by an individual or group that is reasonably suspected of involvement in criminal or terrorist activity, and meets valid criminal intelligence suspicion criteria. Criminal activity shall not include motor vehicle-related offenses.
2. *Criminal intelligence system* means the arrangements, equipment, facilities, and procedures used for the receipt, analysis, storage, interagency sharing, or dissemination of criminal intelligence information.

3. *Information and analysis center* means an organizational entity within the department of safety that compiles, analyzes and disseminates information in support of efforts to anticipate, identify, prevent, mitigate, respond to, and recover from natural and human-caused threats to the state and its people or to the United States, on behalf of the single government agency and also operates an inter-jurisdictional intelligence sharing system on behalf of 2 or more participating agencies, whether called a criminal intelligence system, information and analysis center, fusion center, or by any other name.
4. *Intelligence data* means information and data gathered from a number of sources that, when analyzed and evaluated, provides the basis for decision-making to help ensure the safety and well-being of the people of New Hampshire from actual or impending criminal or terrorist activity.
5. *Inter-jurisdictional intelligence system* means an intelligence system that involves 2 or more participating agencies representing different governmental units or jurisdictions.
6. *Participating agency* means an agency of a local, county, state, federal, or other governmental unit that exercises homeland security, emergency management, law enforcement, or criminal investigation authority and is authorized to submit and receive criminal intelligence data through an inter-jurisdictional intelligence system. A participating agency may be a member or non-member of an inter-jurisdictional intelligence system.
7. *Personally identifiable data* means data or information that contains a person's name, date, place of birth, social security number, address, employment history, credit history, financial information, account numbers, cellular telephone, voice over Internet protocol or landline telephone numbers, biometric identifiers including fingerprints, facial photographs or images, retinal scans, DNA/RNA, or other identifying data unique to that individual.
8. *Reasonably suspected* means information received and evaluated by a law enforcement officer or intelligence analyst in consideration of his or her training and experience and the facts and circumstances under which it was received that would cause a prudent person to conclude that there are sufficient facts to believe that the information is relevant to and will aid in the detection, discovery, or interruption of actual, planned, or impending criminal or terrorist activity by an individual or group.
9. *Validation of information* means the procedures governing the periodic review of criminal intelligence and personally identifiable data to assure its continuing compliance with system submission criteria. (Kurk et al., 2009)

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX F. DRAFT NEW HAMPSHIRE INFORMATION AND ANALYSIS CENTER STRUCTURE

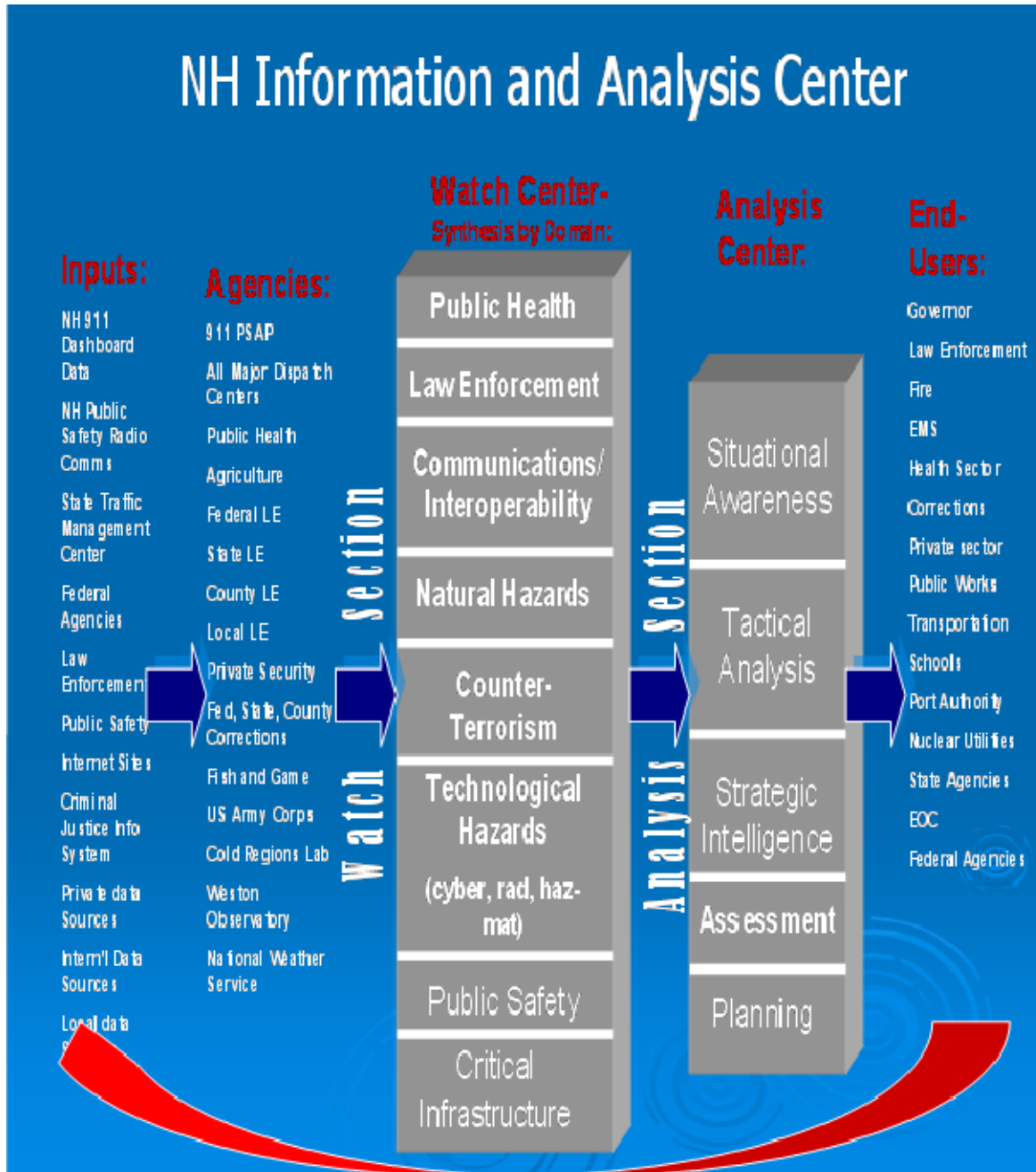


Figure 8. Proposed New Hampshire Information and Analysis Center Structure (From Pope, 2009)

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

- American Civil Liberties Union. (2005, May 11). *ACLU of Massachusetts questions scope of fusion center activities* [press release]. Retrieved August 23, 2009, from <http://www.aclum.org/news/05.11.05.Fusion.pdf>
- American Civil Liberties Union. (2007, December 12). *ACLU Releases New Report on Government "Fusion Centers" in Massachusetts and nationwide* [press release]. Retrieved August 23, 2009, from http://www.aclum.org/news/ACLUM_12_12_07_Fusion_Centers.pdf
- American Civil Liberties Union. (2007, December 12). *New "fusion centers" must be open, carefully monitored and subject to restraints, ACLU Says in New Report* [press release]. Retrieved September 7, 2008, from <http://www.aclu.org/privacy/gen/33170prs20071212.html>
- American Civil Liberties Union. (2008, April 2). *ACLU Urges Senate Judiciary Committee to Probe Department of Homeland Security*. Retrieved August 16, 2008, from <http://www.aclu.org/safefree/general/34744prs20080402.html>
- American Civil Liberties Union. (2008, July 29). *Fusion Centers Part of Incipient Domestic Intelligence System, ACLU Warns*. Retrieved August 5, 2008, from <http://www.aclu.org/safefree/general/36285prs20080729.html>
- American Civil Liberties Union Massachusetts (2009, October 21). *Testimony of Carole Rose, Executive Director, ACLU of Massachusetts in support of SB931 an Act regarding the Commonwealth Fusion Center and other intelligence data centers*. Boston, MA. Retrieved December 9, 2009, from http://aclum.org/sos/aclu_testimony_sb931_crose.pdf
- American Civil Liberties Union Massachusetts (2007, December 12). *ACLU releases new report on government "fusion centers" in Massachusetts and nationwide* [press release]. Boston, MA. Retrieved October 12, 2009, from http://www.aclum.org/news/ACLUM_12_12_07_Fusion_Centers.pdf
- Arizona Department of Public Safety. *Arizona fusion center*. Retrieved December 11, 2009, from http://www.azdps.gov/About/Task_Forces/Fusion/
- Arizona Department of Public Safety. (2008, February 29). *Arizona Counter Terrorism Information Center Privacy and Civil Rights Procedures Guide*.
- Arizona Department of Public Safety. (2008). *Arizona Counter Terrorism Information Center privacy policy*. Phoenix, AZ.

- Bain, B. (2008, October 27). *Guidance for fusion centers to be released*. Retrieved November 8, 2008, from <http://www.fcw.com/online/news/154206-1.html?type=pf>
- Department of Homeland Security, Intelligence and Analysis. (2009). *Baseline Capabilities—Information Privacy Protections Spreadsheet* [internal document].
- Baseline Capabilities for State and Major Urban Area Fusion Centers A Supplement to the Fusion Center Guidelines. (2008, September). U.S. Department of Justice and U.S. Department of Homeland Security. Washington, DC:
- Bureau of Justice Statistics, Office of Justice Programs, Department of Justice. (2003). *Compendium of state security and privacy legislation: Overview 2002*. Washington, DC: author. Retrieved October 2, 2009, from <http://www.ojp.usdoj.gov/bjs/pub/pdf/cspsl02.pdf>
- Carter, D. L. (2008). *The intelligence fusion process*. East Lansing, MI: Michigan State University.
- Carter, D. L. (2009) *Law enforcement intelligence: A guide for state, local, and tribal law enforcement agencies* (2nd ed.). East Lansing, MI: Michigan State University.
- Chandler, Harriette L. (2009, January). *Senate Bill 931 An Act regarding the Commonwealth Fusion Center and other intelligence data centers*. Retrieved December 7, 2009, from <http://www.mass.gov/legis/bills/senate/186/st00pdf/st00931.pdf>
- Commonwealth of Massachusetts, Executive Department (2007, January). *Executive Order No. 476*. Boston, MA. Retrieved August 23, 2009, from <http://archives.lib.state.ma.us/bitstream/handle/2452/46578/ocm18597463-2007-EO476.pdf?sequence=1>
- Commonwealth of Massachusetts, Executive Office of Public Safety and Security. (2006). *Commonwealth Fusion Center Standard Operating Procedure—Privacy Policy CFC-05* [internal document]. Boston: MA: author.
- Commonwealth of Massachusetts, Executive Office of Public Safety and Security (2006). *Commonwealth Fusion Center Operations Manual* [internal document]. Boston: MA: author.
- Commonwealth Fusion Center. (n.d.). *Fusion Center Overview*. Retrieved August 23, 2009, from http://www.mass.gov/?pageID=eopsterminal&L=3&L0=Home&L1=Homeland+Security+%26+Emergency+Response&L2=Commonwealth+Fusion+Center&sid=Eeops&b=terminalcontent&f=msp_homeland_security_terrorism_fusion_center_fusion_center_overview&csid=Eeops

- Coney, L. (2007, September). *Statement, Department of Homeland Security Data Privacy and Integrity Advisory Committee*. Retrieved July 15, 2009, from <http://epic.org/privacy/fusion/fusion-dhs.pdf>
- Department of Homeland Security. (n.d.). *State and local fusion centers*. Retrieved December 6, 2009, from http://www.dhs.gov/files/programs/gc_1156877184684.shtm
- Department of Homeland Security. (2008). *Privacy impact assessment for the Department of Homeland Security state, local, and regional fusion center initiative*. Washington, DC: author.
- Department of Homeland Security. (2007). *Target Capabilities List A Companion to the National Preparedness Guidelines*. Washington, DC: authors. Retrieved on September 12, 2009, from <http://www.fema.gov/pdf/government/training/tcl.pdf>
- Department of Homeland Security & Department of Justice. (2006). *Fusion Center Guidelines Developing and Sharing Information and Intelligence in a New Era*. Washington, DC: authors.
- Forsyth, W.A. (2005). *State and local intelligence fusion centers: An evaluative approach in modeling a state fusion center*. Master's thesis, Naval Post Graduate School, Monterey, CA.
- Fusion center model privacy policy—Sample template*. (2004, December) Retrieved August 23, 2009, from www.llis.dhs.gov
- German, M. & Stanley, J. (2007, December). *What's wrong with fusion centers?* Retrieved October 15, 2008, from http://www.aclu.org/pdfs/privacy/fusioncenter_20071212.pdf
- Georgia Bureau of Investigation. (2008). *Directive 7-6 Criminal Intelligence Operations and Privacy Protections* [internal document]. Atlanta, GA: Investigative Division, Georgia Bureau of Investigation.
- Georgia Emergency Management Agency. (n.d.). *Georgia emergency management agency*. Retrieved September 5, 2009, from <http://www.gema.ga.gov/ohsgemaweb.nsf/>
- Global Justice Information Sharing Initiative, Office of Justice Programs, Department of Justice. (2003). *National Criminal Intelligence Sharing Plan*. Washington, DC: Department of Justice & Bureau of Justice Assistance.
- Global Justice Information Sharing Initiative, Office of Justice Programs, U.S. Department of Justice. (2008a). *Privacy, civil liberties, and information: Quality policy development for the justice decision maker*. Retrieved March 14, 2009, from http://it.ojp.gov/documents/global_privacy_brief.pdf

- Global Justice Information Sharing Initiative, Office of Justice Programs, U.S. Department of Justice. (2008b). *Privacy and civil liberties policy development guide and implementation templates*. Retrieved April 5, 2009, from http://www.it.ojp.gov/documents/Privacy_Guide_Final.pdf
- Harper, J. (2007, March 13). *Fusion centers: Leave 'em to the states*. Retrieved August 1, 2009, from <http://www.cato.org/tech/tk/070314-tk.html>
- Program Manager, Information Sharing Environment. *Information sharing environment implementation plan*. (2006). Washington, DC: Office of the Director of National Intelligence.
- Kayyem, Juliette N. *Undersecretary for Homeland Security Commonwealth of Massachusetts*. "Moving beyond the first five years: Evolving the Office of Intelligence and Analysis to better serve state, local, and tribal needs." *Testimony before the Subcommittee on Intelligence, Information Sharing and Terrorism Risk Assessment*. (2008). Retrieved October 23, 2009, from <http://homeland.house.gov/SiteDocuments/20080424101941-64603.pdf>
- Kurk, N. & Burrridge, D. (2009, January 8) *New Hampshire House Bill 587 establishing an information and analysis center within the department of safety*. Retrieved August 14, 2009, from <http://www.gencourt.state.nh.us/legislation/2009/HB0587.html>
- Longoria, B. (2009, September 8). "Fusion center" meets criticism from local ACLU. *The Daily Texan*. Retrieved October 2, 2009, from <http://www.dailytexanonline.com/top-stories/fusion-center-meets-criticism-from-local-aclu-1.1868856>
- Lowenthal, M. (2006). *Intelligence: From Secrets to Policy* (3rd ed.). Washington, DC: CQ Press.
- Massee, T, O'Neil, S., & Rollins, J. (2007). *Fusion Centers: Issues and Options for Congress* (RL34070). Washington, DC: Congressional Research Service.
- Massee, T. & Rollins, J. (2007, September 19). *A Summary of Fusion Centers: Core Issues and Options for Congress*. Washington, D.C.: Congressional Research Service, RL34177.
- Merriam Webster Editorial Staff (2003). *Privacy. Merriam-Webster's Collegiate Dictionary*: (11th ed.). Portland, OR. Book News, Inc.
- National Commission on Terrorist Attacks upon the United States. (2007). *The 9/11 Commission Report: The final report of the National Commission on Terrorist Attacks Upon the United States*. New York: W.W. Norton & Company, Inc., First Edition.

- National Governor's Association Center for Best Practices. (2005). *Issue brief: Establishing State Intelligence Fusion Centers*. Washington, DC: Retrieved September 12, 2009, from <http://www.nga.org/Files/pdf/FusionCenterIB.pdf>
- National Research Council. (2008). *Protecting individual privacy in the struggle against terrorists*. Washington, DC: The National Academies Press.
- New Hampshire Constitution. (1784). Retrieved May 20, 2009, from <http://www.nh.gov/constitution/billofrights.html>
- New Hampshire Department of Safety, Division of Homeland Security and Emergency Management. (2008). New Hampshire Emergency Management Performance Grant [internal document]. Concord, NH: author.
- New Hampshire Revised Statutes Annotated. (1977). Section 91–A:1, preamble. Retrieved May 20, 2009, from <http://www.gencourt.state.nh.us/rsa/html/VI/91-A/91-A-mrg.htm>
- New Hampshire Revised Statutes Annotated. (2008a). Section 91–A:5. Retrieved May 20, 2009, from <http://www.gencourt.state.nh.us/rsa/html/VI/91-A/91-A-mrg.htm>
- New Hampshire Revised Statutes Annotated. (2008b). Section 91–A:5–V17. Retrieved May 20, 2009, from <http://www.gencourt.state.nh.us/rsa/html/VI/91-A/91-A-mrg.htm>
- New Hampshire Revised Statutes Annotated. (2008c). Section 91–A:1–a definitions. Retrieved May 20, 2009, from <http://www.gencourt.state.nh.us/rsa/html/VI/91-A/91-A-mrg.htm>
- Office of Inspector General, Department of Homeland Security (2008). DHS' Role in State and Local Fusion Centers Is Evolving. (2008, December). U.S. Department of Homeland Security, Office of the Inspector General. OIG-09-12, Washington, D.C.
- Office for Civil Rights and Civil Liberties & Privacy Office, Department of Homeland (2008). *28 CFR Part 23*, Retrieved on April 5, 2009, from <http://it.ojp.gov/default.aspx?area=privacy&page=1260>
- Pope, Christopher (2009). *Draft New Hampshire Information and Analysis Center Structure*. Concord, NH: New Hampshire Department of Safety, Division of Homeland Security and Emergency Management.
- Riegle, Robert (2008, July). Cultivating Relationships: A view of DHS' state & local program at age three. *Homeland Defense Journal*

- Rogers, Richard. (2008). Reality Check: Undermining a crucial law enforcement tool. *Identity Theft 911 Newsletter* 5(6). Retrieved April 4, 2009, from <http://identitytheft911.org/newsletters/index.htm>
- Rollins, John (2008 January). *Fusion Centers: Issues and Options for Congress*. Washington, D.C.: Congressional Research Service, RL34070.
- Rollins, J. & Connors, T. (2007). State Fusion Center Processes and Procedures: Best Practices and Recommendations. *Policing Terrorism Report* 2.
- Stelter, L. (2009, September 11). "9/11: A day for reflection." *Security Director News*. Retrieved September 19, 2009, from <http://www.securitydirectornews.com/?p=article&id=sd200909S0jzw5>
- Teufel, Hugo, III, Chief Privacy Officer, U.S. Department of Homeland Security. *Testimony before the Committee on Homeland Security Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment*. (2007). Retrieved December 10, 2009, from <http://hsc.house.gov/SiteDocuments/20070314172345-08973.pdf>
- Treverton, G. (2008). *Reorganizing U.S. Domestic Intelligence: Assessing the Options*. Santa Monica, CA: RAND Corporation.
- U.S. Government Accountability Office. (2008). *Testimony before the Ad Hoc Subcommittee on State, Local, and Private Sector Preparedness and Integration, Committee on Homeland Security and Government Affairs, U.S. Senate: Homeland security federal efforts are helping to alleviate some challenges encountered by state and local information fusion centers* (GAO-08-636T). Washington, DC: author. Retrieved on September 12, 2009, from <http://www.gao.gov/new.items/d08636t.pdf>
- U.S. Government Accountability Office. (2007). *Homeland security federal efforts are helping to alleviate some challenges encountered by state and local information fusion centers* (GAO-08-35). Washington, DC: author. Retrieved on September 12, 2009, from <http://www.gao.gov/new.items/d0835.pdf>.
- Wasted lessons of 9/11: How the Bush administration has ignored the law and squandered its opportunities to make our country safer*. (2008). Washington, DC: Committee on Homeland Security & Committee on Foreign Relations, U.S. House of Representatives. <http://homeland.house.gov/SiteDocuments/HR1AnniversaryReport.pdf>
- White House. (2007). *National Strategy for Information Sharing - Successes and Challenges In Improving Terrorism-Related Information Sharing*. Washington, DC: author.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
Ft. Belvoir, Virginia
2. Dudley Knox Library
Naval Postgraduate School
Monterey, California
3. Christopher M. Pope, Director
New Hampshire Department of Safety, Division of Homeland Security and
Emergency Management
Concord, New Hampshire
4. Kathryn E. Douth, Assistant Director
New Hampshire Department of Safety, Division of Homeland Security and
Emergency Management
Concord, New Hampshire
5. John J. Barthelmes, Commissioner
New Hampshire Department of Safety
Concord, New Hampshire
6. Earl Sweeney, Assistant Commissioner
New Hampshire Department of Safety
Concord, New Hampshire